Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA –COLOMBIA COMPRA EFICIENTE-

2026

Directora General (E)
Ana María Tolosa Rico

Secretaria General
Ana María Tolosa Rico

Subdirectora de Negocios
Yenny Liseth Pérez Olaya

Subdirectora de Gestión Contractual
Carolina Quintero Gacharná

Subdirector de Información y Desarrollo Tecnológico (IDT)
Richard Ariel Bedoya De Moya

Subdirector (E) de Estudios de Mercado y Abastecimiento Estratégico (EMAE)
Richard Ariel Bedoya De Moya

Asesora Experta de Despacho
Sindy Alexandra Quintero Hernández

Asesor Experto de Despacho
Luis Enrique Perea Garcés

Asesor Experto de Despacho
William Javier Murcia Acevedo

Asesora de Control Interno
Edith Cárdenas Herrera

TABLA DE CONTENIDO

1. OBJETIVO 8
2. ALCANCE 8
3. TERMINOS Y DEFINICIONES 9
4. MARCO DE REFERENCIA ESPECÍFICO 15
5. REFERENCIAS NORMATIVAS 16
6. ESTRUCTURA ORGANIZACIONAL DEL SUBSISTEMA DE GESTIÓN 17
Ilustración 1:Organigrama Seguridad de la Información 17
7. POLÍTICA DE ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 17
7.1. Responsabilidades de la Alta Dirección a través del COASIC 18
7.2. Responsabilidades del(os) Dueño(s) de Proceso(s) y Administrador(es) de los Sistemas de Información 19
7.3. Subdirector de Información y Desarrollo Tecnológico 21
7.4. Responsabilidades de la Coordinación de Seguridad e Infraestructura de la ANCP-CCE 22
7.5. Responsabilidad del Asesor, Contratista u Oficial (o quién haga sus veces) designado para la Privacidad y la Protección de Datos Personales 24
8. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 25
8.1. Componente de Política de Gobierno 26
8.1.1. Políticas para la seguridad de la información 26
8.1.2. Roles y responsabilidades de seguridad de la información 28
8.1.3. Segregación de funciones 30
8.1.4. Gestión de responsabilidades 34
8.1.5. Contacto con autoridades 42
8.1.6. Contacto con grupos de interés especiales 44
8.1.7. Seguridad de la información en la gestión de proyectos 46
8.2. Componente Política de Administración de amenazas y vulnerabilidades 50
8.2.1. Inteligencia de amenazas 50

8.2.2. Gestión de vulnerabilidades técnicas 54
8.3. Componente Política de Administración de activos..... 62
8.3.1. Inventario de información y otros activos asociados..... 62
8.3.2. Uso aceptable de la información y otros activos 67
8.3.3. Devolución de activos 74
8.4. Componente Política de Protección de Información..... 77
8.4.1. Clasificación de la información 77
8.4.2. Etiquetado de la información..... 81
8.4.3. Transferencia de información 85
8.4.4. Derechos de propiedad intelectual (IPR) 95
8.4.5. Protección de registros 101
8.4.6. Privacidad y protección de información personal identificable (PII) 106
8.4.7. Trabajo a distancia..... 111
8.4.8. Dispositivos terminales de usuario 118
8.4.9. Supresión de información..... 126
8.4.10. Enmascaramiento de datos..... 129
8.4.11. Prevención fuga de datos 132
8.4.12. Información de prueba..... 135
8.4.13. (8.34) Protección de sistemas de información durante pruebas de auditoría 138
8.5. Componente Política de Control de acceso 139
8.5.1. Acceso a la información 139
8.5.2. Gestión de identidad..... 143
8.5.3. Información de autenticación 146
8.5.4. Derechos de acceso..... 151
8.5.5. Derechos de acceso privilegiado 156
8.5.6. Restricción de acceso a la información..... 160
8.5.7. Acceso a código fuente 163
8.5.8. Autenticación segura 167

8.6. Componente Política de Proveedores 171
8.6.1. Seguridad de la información en relaciones con proveedores 171
8.6.2. Acuerdos con proveedores 182
8.6.3. Gestión de seguridad de la cadena de suministro TIC 186
8.6.4. Supervisión de servicios de proveedores 191
8.6.4.1. Uso de servicios en la nube 196
8.7. Componente Política de gestión de Eventos 205
8.7.1. Gestión de incidentes de seguridad de la información 205
8.7.2. Evaluación de eventos de seguridad 210
8.7.3. Respuesta ante incidentes de seguridad de la información 213
8.7.4. Aprendizaje a partir de incidentes de seguridad 217
8.7.5. Informe de eventos de seguridad de la información 223
8.7.6. Registro 225
8.7.7. Actividades de monitoreo 229
8.7.8. Sincronización de reloj 236
8.8. Componente Política de Continuidad 238
8.8.1. Recolección de evidencia 238
8.8.2. Continuidad de la seguridad de la información 245
8.8.3. Gestión de capacidad 249
8.8.4. Respaldo de información 253
8.8.5. Redundancia de instalaciones de tratamiento de información 262
8.9. Componente Política de legal y Cumplimiento 265
8.9.1. Cumplimiento de requisitos legales, estatutarios y contractuales 265
8.10. Componente Política de Revisión Independiente 268
8.10.1. Revisión independiente de la seguridad de la información 268
8.11. Componente Política de Seguridad Recursos Humanos 270
8.11.1. Comprobación de antecedentes de todos los candidatos 270
8.11.2. Términos y condiciones de trabajo 272
8.11.3. Concientización, educación y capacitación en seguridad de la información 275

8.11.4. Proceso disciplinario 277
8.11.5. Responsabilidades después de la terminación o cambio de empleo 278
8.11.6. Acuerdos de confidencialidad o no divulgación 282
8.12. Componente Política de Seguridad Física 285
8.12.1. Perímetros de seguridad física..... 285
8.12.2. Acceso físico 288
8.12.3. Aseguramiento de oficinas, salas e instalaciones 292
8.12.4. Supervisión de seguridad física 295
8.12.5. Protección contra amenazas físicas y medioambientales 298
8.12.6. Trabajo en zonas seguras..... 303
8.12.7. Escritorio y pantalla despejados 309
8.12.8. Ubicación y protección de equipos 314
8.12.9. Seguridad de activos fuera de las instalaciones..... 322
8.12.10. Medios de almacenamiento..... 326
8.12.11. Servicios de apoyo 332
8.12.12. Seguridad de cableado..... 335
8.12.13. Mantenimiento de equipo 339
8.13. Componente Política de Seguridad de Redes 345
8.13.1. Protección contra "malware"..... 345
8.13.2. Seguridad de redes 351
8.13.3. Seguridad de servicios de red 362
8.13.4. Segregación de redes 364
8.13.5. Filtro Web..... 367
8.14. Componente Política de Seguridad de Configuraciones..... 372
8.14.1. Gestión de configuración 372
8.14.2. Uso de criptografía..... 376
8.15. Componente Política de Seguridad de Aplicaciones..... 384
8.15.1. Uso de programas privilegiados de utilidad: 384
8.15.2. Ciclo de vida de desarrollo seguro..... 387

8.15.3. Requisitos de seguridad de las aplicaciones 390
8.15.4. Principios de ingeniería y arquitectura de sistemas seguros..... 397
8.15.5. Codificación segura: 401
8.15.6. Pruebas de seguridad en desarrollo y aceptación..... 406
8.15.7. Desarrollo externo: 410
8.15.8. Separación de entornos de desarrollo, prueba y producción 412
8.15.9. Gestión de cambios 418
8.16. Política De Tratamiento Y Protección De Datos..... 425
9. GESTIÓN DE RIESGOS 425
10. INDUCCIÓN, CAPACITACIÓN Y DESARROLLO DE COMPETENCIAS ... 426
10.1. Inducción 427
10.2. Capacitación Continua 427
10.3. Sensibilización y Comunicación 427
10.4. Entrenamiento Especializado 428
10.5. Evaluación y Mejora Continua 428
10.6. Integración con el PIC 428
11. PREPARACION Y RESPUESTA ANTE EMERGENCIAS 428
11.1. Alcance 429
11.2. Identificación y evaluación de escenarios de emergencia..... 430
11.3. Preparación para la respuesta..... 430
11.4. Clasificación de la emergencia 431
11.5. Activación de la respuesta..... 432
11.6. Respuesta ante emergencias 433
11.7. Gestión de la información durante la emergencia 434
11.8. Comunicación durante la emergencia..... 434
11.9. Recuperación y retorno a la operación normal 435
12. CONTROL DE PROVEEDORES Y CONTRATISTAS..... 435
13. MEDICIÓN Y SEGUIMIENTO 436
14. GESTIÓN DE CAMBIOS..... 436

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE ILUSTRACIONES

Ilustración 1: Organigrama Seguridad de la Información 17
Ilustración 2: Roles y responsabilidades ante emergencias..... 65
Ilustración 3: Clasificación de emergencias..... 66

TABLA DE TABLAS

Tabla 1: matriz de segregación de funciones 33

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Establecer los lineamientos para proteger la información gestionada por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente en adelante ANCP-CCE, garantizando su confidencialidad, integridad, disponibilidad, privacidad y no repudio. Su propósito es apoyar el cumplimiento de los objetivos estratégicos de la entidad, fortaleciendo la gestión pública mediante un Sistema de Gestión de Seguridad de la Información (SGSI) como parte del Sistema Integrado de Gestión (SIG), promoviendo la mejora continua y la protección de los activos de información.
Este manual se enmarca en el Modelo de Seguridad y Privacidad de la Información (MSPI) y responde a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las políticas de Gobierno Digital.

2. ALCANCE

Hace parte del alcance del presente Manual, toda la información creada, procesada y/o utilizada por la ANCP- CCE en todas sus formas independientemente del medio (digital, manuscrita, fonética, impresa), presentación y/o lugar en el cual se encuentre ubicada.

Es así como, lo establecido en el presente documento, anexos y/o posteriores actualizaciones es aplicable y de obligatorio cumplimiento para:

- Toda la Entidad, sus órganos de dirección, funcionarios públicos, contratistas, proveedores y todas aquellas personas y/o terceros que debido al cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien y/o consulten información de la Entidad.
- Las Entidades de control y demás Entidades relacionadas que accedan a cualquier Activo de Información propiedad de la ANCP-CCE, independientemente de su ubicación.
- Los procesos internos que traten Activos de información en cumplimiento de sus objetivos estratégicos.

3. TERMINOS Y DEFINICIONES

Activo de Información: Es la información que reside en medio electrónico o físico, que tiene un significado y valor para ANCP-CCE y por tanto requiere protección.

Acuerdo de Nivel de Servicio: Es el estándar de calidad de la prestación de un servicio fijado por el proveedor del servicio y su cliente.

Algoritmo de Cifrado: Secuencia de instrucciones matemáticas usadas para transformar textos o datos legibles y entendibles en textos o datos cifrados y viceversa.

Ambiente: Conjunto de elementos o componentes tecnológicos o, grupos de sistemas de información, en los cuales reside o fluye información y datos de negocio.

Aplicación Endpoint: Software cuya función es detectar y/o eliminar aplicaciones maliciosas informáticas.

Backup: Es la copia de respaldo de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

Cifrado de datos: Procedimiento mediante el cual la información legible se transforma en información ilegible (cifrada) y solo se puede volver legible nuevamente con la clave o llave con la que se cifraron los datos.

Cinta LTO (Linear Tape-Open): Es una tecnología de cinta magnética de almacenamiento de datos, desarrollada como alternativa de estándares abiertos a los formatos de cinta magnética. LTO es ampliamente utilizado con los sistemas informáticos pequeños y grandes, sobre todo para copias de seguridad.

Cláusula de Confidencialidad: Es la obligación establecida en un contrato para establecer las condiciones en las cuales la información que conozcan las partes con ocasión de la ejecución del contrato puede y debe ser divulgada.

COASIC: Comité de Apoyo de Seguridad de la Información y Ciberseguridad

Confidencialidad: Es el principio de la Seguridad de la Información que busca asegurar que la información de la Entidad sea accedida únicamente por el personal autorizado para el efecto.

Contraseña: Conjunto de caracteres alfanuméricos que permiten a un usuario el acceso a un determinado recurso o la utilización de un servicio.

Control Dual: Consiste en entregar a dos diferentes custodios las partes de una llave criptográfica o contraseña.

Correo No Deseado: Mensaje de correo basura no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
Criptografía: Conjunto de técnicas (algoritmo, protocolo y/o mecanismo) que buscan proteger y preservar la confidencialidad, integridad y autenticidad de la información de observadores no autorizados.
Custodia Física o Digital: Es la acción de proteger la información teniendo cuenta los principios de confidencialidad, integridad y disponibilidad.

Dato Personal: Es cualquier e dato que identifique o permita la identificación de una persona natural.

Dato Personal privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato Personal semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general

Dato Personal sensible: Es aquel Dato Personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación.

Disponibilidad: Es el principio de la Seguridad de la Información que busca asegurar que la información sea accesible y utilizable cuando sea requerida.

Escaneo de Vulnerabilidades: proceso que ejecuta una solución tecnológica determinada para identificar las vulnerabilidades que presenta un componente de infraestructura tecnológica.

Firma Digital: Esquema matemático que sirve para demostrar la autenticidad de un mensaje digital.

Gestión de Llaves Criptográficas: La gestión de llaves criptográficas contempla las actividades de crear, ingresar, eliminar, modificar (actualizar), verificar, definir custodios e inventariar.

Implementación del Servicio: Todas las actividades necesarias para hacer disponible un servicio sobre infraestructura local o en la nube.

Incidente de Seguridad: Es cualquier evento que compromete la integridad, confidencialidad o disponibilidad de la información o de los sistemas de información de una organización. Estos incidentes pueden incluir accesos no autorizados, ataques cibernéticos (como malware, ransomware, phishing,

ataques DoS/DDoS), pérdida o robo de datos, violaciones de políticas de seguridad, fallos técnicos en hardware, software o red, y errores humanos que comprometen la seguridad, como enviar información confidencial a la persona equivocada.

Información Confidencial: Es la información que tiene restricciones para su uso y que puede estar etiquetada como "Clasificada" o "Reservada".

Integridad: Es el principio de Seguridad de la Información para evitar su modificación o alteración y garantizar su consistencia, exactitud y completitud.

Llave Criptográfica: Secuencia de números y/o letras que controlan el comportamiento de un algoritmo de cifrado.

Logs de Auditoría: Este tipo de Log registra las operaciones Gestión Administrativas que se realicen o ejecuten sobre los componentes o aplicaciones de la infraestructura tecnológica generando una traza de eventos auditables.

Mesa de Ayuda: Es el grupo encargado de apoyar en administración y solución de problemas tecnológicos internos propios de Colombia Compra Eficiente.

Mesa de Servicio: Área encargada de atender los requerimientos y solicitudes de todos los partícipes de la compra pública.

Modelo de Seguridad y Privacidad de la Información (MSPI): Modelo orientado a la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación y Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Nube (Cloud): Disponibilidad de recursos de computación bajo demanda (como almacenamiento e infraestructura) como servicios a través de Internet.

No Repudio: Es la irrenunciabilidad, es decir, permite probar la participación de las diferentes partes en una comunicación.

OneDrive: Es un servicio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.

Oficial de Seguridad de la Información: Es el contratista y/o funcionario que cumple la función de supervisión del cumplimiento del MSPI y la Seguridad Digital dentro de la Entidad.

Plan de Continuidad de Negocio: Es el plan para restaurar las funciones críticas de la Entidad de forma parcial o totalmente para recuperar sus Activos de Información luego de una interrupción no deseada o un desastre.

Plan de Seguridad y Privacidad de la Información (PSPI): Comprende todas aquellas actividades que contribuyen a la protección de la información.

Política de Seguridad: Es una declaración formal de las reglas, directivas y prácticas que rigen la forma de gestión de los activos de tecnología e información dentro de una organización.

Principio de Menor Privilegio: Es una estrategia de seguridad, aplicable a distintos ámbitos, que se apoya en la idea de otorgar únicamente permisos cuando son necesarios para el desempeño de cierta actividad.

Privacidad: Consiste en garantizar que solo aquellos que están autorizados a acceder a los datos puedan hacerlo.

Procesamiento de Datos: Serie de operaciones que utilizan información para producir un resultado, de esta forma se recolectan de los datos primarios de entrada, que son evaluados y ordenados, para obtener información útil, que luego serán analizados por el usuario final, para que pueda tomar las decisiones o realizar las acciones que estime conveniente.

Pruebas de Penetración: Proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y redes informáticas cuyo objetivo es encontrar las debilidades tecnológicas y así prevenir la posibilidad que ocurra una actividad maliciosa interna o externa.

Recurso Tecnológico: Es cualquier medio tecnológico de Colombia Compra Eficiente.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad de la Información: Es el conjunto de medidas que busca preservar la Confidencialidad, la Integridad y la Disponibilidad de la información.

SGSI: Es el Sistema de Gestión de Seguridad de la información conformado por un conjunto de elementos, prácticas y procesos para implementar, operar, mantener y mejorar la Seguridad de la Información.

Sistema de Información: Es el conjunto de elementos que interactúan para apoyar los objetivos de un negocio como por ejemplo la información, actividades, hardware, software entre otros.

Subdirección de IDT: Es la Subdirección de Información y Desarrollo Tecnológico de Colombia Compra Eficiente.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Uso aceptable: Administración responsable, ética y legal de cada uno de los activos de información.

Usuario: Es la persona que utiliza el servicio de tecnología contratado.

Virus Informático: Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

Vulnerabilidad: es una debilidad en un sistema o componente tecnológico, que puede ser explotada por una amenaza para materializar un riesgo.

4. MARCO DE REFERENCIA ESPECÍFICO

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en Colombia Compra Eficiente se fundamenta en la adopción de buenas prácticas institucionales y modelos de gestión que promueven la eficiencia, la transparencia y la protección de la información. Este marco de referencia se articula con:

- El Sistema Integrado de Gestión (SIG) de la entidad, como herramienta para fortalecer la calidad y coherencia de los procesos internos.
- El Modelo Integrado de Planeación y Gestión (MIPG), que orienta la gestión pública hacia el cumplimiento de objetivos institucionales con enfoque en resultados.
- El Modelo de Seguridad y Privacidad de la Información (MSPI), promovido por el MinTIC, como guía para establecer controles que aseguren la confidencialidad, integridad, disponibilidad, privacidad y no repudio de la información.
- Las políticas internas de mejora continua y gestión del riesgo, que permiten anticipar y mitigar amenazas que puedan comprometer los activos de información.
- En concordancia con la Política Nacional de Gobierno Digital, adoptada mediante el CONPES 3995 de 2020, la Agencia ha definido y adoptado su propia Política Interna de Gobierno Digital, aprobada mediante acto

administrativo interno. Esta política adapta y complementa los lineamientos nacionales a las particularidades organizacionales, operativas y estratégicas de la entidad. En ella se establecen directrices específicas para la implementación de componentes clave como la arquitectura empresarial, la gestión de datos, la interoperabilidad y, de manera destacada, la arquitectura de seguridad digital, la cual se articula con el MSPI como instrumento técnico para garantizar la protección de los activos de información.

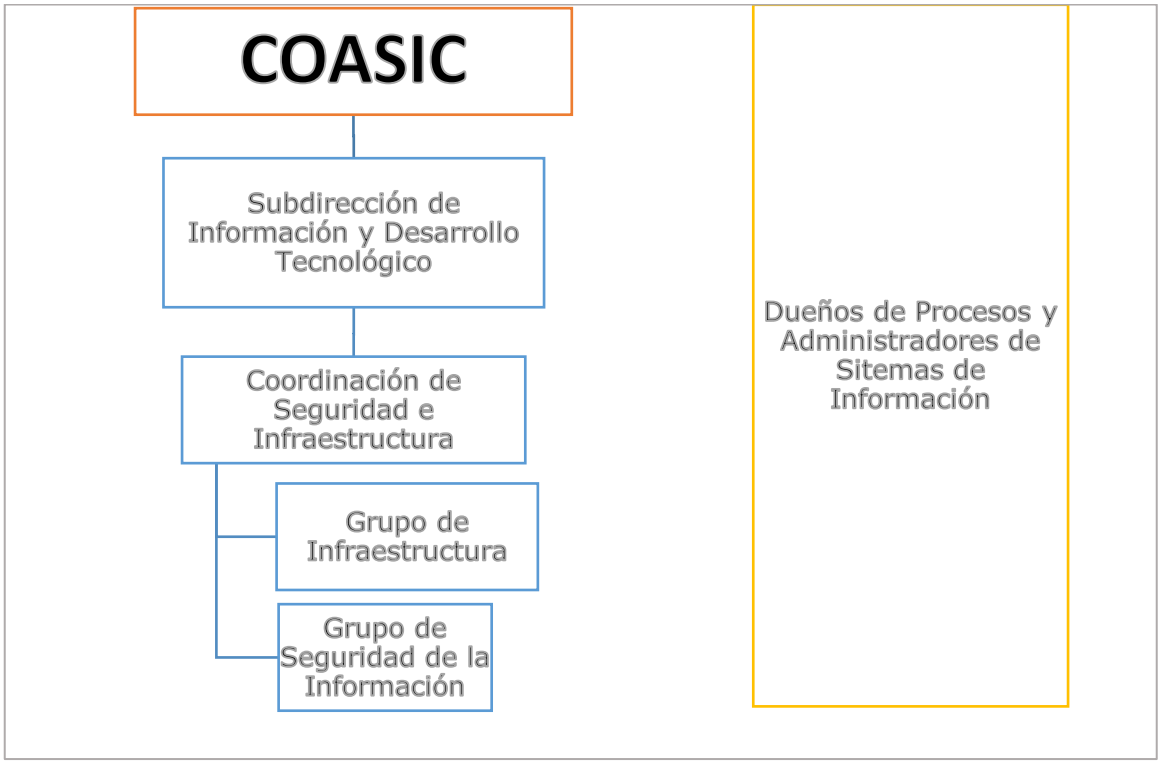
Este marco permite alinear la gestión de la seguridad de la información con la misión institucional, garantizando que los servicios y productos ofrecidos respondan a las necesidades de los ciudadanos y demás partes interesadas.

5. REFERENCIAS NORMATIVAS

Ver en el Normograma asociado al proceso Gestión de Tecnologías de Información en el siguiente enlace [Normograma ANCP-CCE]

6. ESTRUCTURA ORGANIZACIONAL DEL SUBSISTEMA DE GESTIÓN

Ilustración 1:Organigrama Seguridad de la Información



Fuente: elaboración propia

7. POLÍTICA DE ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actualmente, la estructura organizacional del subsistema de gestión de seguridad y privacidad de la información en la ANCP-CCE se encuentra conformada por el Comité de Apoyo de Seguridad de la Información y Ciberseguridad (COASIC), la Subdirección de Información y Desarrollo Tecnológico (IDT), la Coordinación de Seguridad e Infraestructura, y los grupos de trabajo de seguridad, nube y on-premise. Aunque el Grupo de Seguridad de la Información se encuentra actualmente bajo la misma coordinación que infraestructura, se recomienda a futuro considerar su separación como una

unidad independiente o con dependencia directa del COASIC o de la Alta Dirección, en línea con las mejores prácticas del MSPI y la ISO/IEC 27001:2022, que promueven la independencia funcional del rol de seguridad para garantizar su objetividad y capacidad de supervisión transversal.
Esta recomendación busca fortalecer la gobernanza de la seguridad de la información, mejorar la capacidad de respuesta ante incidentes y asegurar una adecuada segregación de funciones entre quienes implementan controles técnicos y quienes los supervisan.

Las responsabilidades frente a la Seguridad y Privacidad de la Información para la alta dirección, los usuarios y para los administradores de los componentes funcionales y técnicos de la ANCP-CCE, definidas dentro de la Política de Seguridad y privacidad de la información son:

7.1. Responsabilidades de la Alta Dirección a través del COASIC

Desde la Alta Dirección de la entidad, se debe apoyar de manera estratégica y transversal la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.

En este marco, se conformó el Comité de Apoyo de Seguridad de la Información y Ciberseguridad (COASIC), cuyos miembros son de la alta dirección, y está formalizado en la resolución 666 de 2023.

Por lo anterior el COASIC tiene como responsabilidades:

- Coordinar, asesorar y apoyar la definición de lineamientos y políticas generales de seguridad de la información y ciberseguridad.
- Recomendar medidas estratégicas para prevenir, detectar, resistir y recuperarse de amenazas a los sistemas informáticos y la infraestructura digital.
- Proponer acciones para fortalecer capacidades institucionales en la gestión de riesgos de seguridad digital.
- Revisar, aprobar y monitorear políticas, procedimientos y planes

relacionados con el SGSI, el MSPI, la continuidad del negocio (BCP) y la recuperación ante desastres.

- Actuar como órgano consultivo en la implementación de planes de continuidad y recuperación.
- Establecer lineamientos y recomendaciones para la ejecución del MSPI y la continuidad de operaciones críticas.
- Revisar y validar informes sobre seguridad y privacidad de la información.
- Presentar quejas o denuncias ante incumplimientos de políticas de seguridad.
- Recomendar recursos humanos y tecnológicos para fortalecer la ciberseguridad institucional.
- Aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Mantener informada a la Alta Dirección sobre eventos críticos o relevantes en materia de seguridad digital.

7.2. Responsabilidades del(os) Dueño(s) de Proceso(s) y Administrador(es) de los Sistemas de Información

- Preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información de la ANCP-CCE.
- Identificar los activos de la información utilizando la matriz ***CCE-GTI-FM-43 Matriz de activos de la información e índice de información reservada y clasificada,*** evaluando su criticidad dentro de la ANCP-CCE, incluyendo los requerimientos de confidencialidad, integridad y disponibilidad
- Clasificar la información de la ANCP-CCE y definir el grupo de usuarios

que deben tener acceso a ella, así como el otorgamiento de los permisos de lectura, escritura y ejecución.

- Definir los marcos de tiempo aceptables para recuperar la información y sistemas críticos de la ANCP-CCE, mediante la definición del RTO y RPO de cada proceso, así como, identificar los impactos institucionales en caso de una interrupción extendida del servicio y/o un ataque.
- Definir la continuidad del objeto misional de la ANCP-CCE mediante el establecimiento de planes de contingencia, continuidad del negocio y requerimientos de recuperación en caso de desastre, siguiendo los recomendaciones de Copias de Respaldo establecidas en este documento.
- Realizar una evaluación continua, con revisiones trimestrales o por cambios significativos, para garantizar la mejora continua y mantener la confidencialidad, integridad y disponibilidad de la información en la ACNP-CCE.
- Definir los requerimientos de seguridad en términos del negocio para que el líder técnico o de Procesos a nivel de Sistema de Información esté en capacidad de proporcionar un nivel adecuado de protección a sus documentos, datos y aplicaciones críticas de conformidad con los estándares y procedimientos de seguridad.
- Definir y autorizar los privilegios de acceso a la información de la ANCP-CCE.
- Incluir los requerimientos de seguridad de información y entrenamiento para la creación de la cultura de seguridad y privacidad de la información dentro de la entidad.
- Liderar el análisis y la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de la información de los sistemas de la ANCP-CCE, incluyendo los incumplimientos a la confidencialidad

y/o integridad de la información.

-

7.3. Subdirector de Información y Desarrollo Tecnológico

- Definir los lineamientos y procesos de arquitectura tecnológica en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación, soporte especializado y mantenimiento.
- Prestar el soporte técnico básico o de primer nivel a los usuarios internos de la entidad garantizando el adecuado funcionamiento de la infraestructura tecnológica base.
- Realizar estudios, diagnósticos, análisis estadísticos y en general recaudar y evaluar la información sobre los aspectos tecnológicos de la compra pública, y promover la articulación de los distintos aspectos legales y reglamentarios en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Diseñar y poner en marcha el plan estratégico de tecnologías de la información.
- Diseñar y proponer las bases técnicas para la contratación electrónica del sector público.
- Definir los estándares de datos de los sistemas de información y de seguridad informática.
- Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la Entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información.
- Gestionar e implementar los instrumentos tecnológicos que se requieren para los mecanismos de adquisición y de agregación de demanda, incluidos los Acuerdos Marco y las subastas, entre otros.
- Absolver consultas de carácter general sobre asuntos de competencia del área.
- Desarrollar e implementar los instrumentos tecnológicos que faciliten a los oferentes una mayor y mejor participación en los procesos de compra pública de las Entidades Estatales, en coordinación con las demás dependencias de Colombia Compra Eficiente.

- Gestionar y administrar el Sistema Electrónico para la Compra pública - SECOP, o el que haga sus veces.
- Realizar las actividades para la integración del SECOP, o del sistema que haga sus veces, con el Registro Único Empresarial de las Cámaras de Comercio y los demás sistemas de gestión cuando así se requiera.
- Proponer mecanismos para articular el SECOP con los sistemas electrónicos públicos que contengan información relacionada con el objeto de Colombia Compra Eficiente.
- Realizar las capacitaciones en materia de compra pública electrónica con el apoyo de las demás áreas de Colombia Compra Eficiente y otras Entidades, cuando así se requiera.
- Proponer estrategias que permitan optimizar el aprovechamiento de la tecnología, la información y las comunicaciones en Colombia Compra Eficiente.
- Apoyar el desarrollo y sostenimiento del Modelo Integrado de Planeación y Gestión de la entidad.
- Aplicar el modelo de control interno de gestión institucional en el desarrollo de las funciones a su cargo.
- Atender y tramitar las peticiones y requerimientos que correspondan a su cargo y función dentro de Colombia Compra Eficiente.
- Presentar oportunamente los informes que le sean requeridos por las autoridades competentes, los organismos de control y las dependencias de Colombia Compra Eficiente.
- Ejercer actividades de supervisión de los contratos que le sean asignados, con el fin de facilitar el logro de los objetivos y estrategias institucionales dando cumplimiento a las normas legales vigentes.
- Dar cumplimiento al Código de Integridad, Código de Convivencia y Código de Ética y Prevención de Conflictos de Interés de la Agencia.

7.4. Responsabilidades de la Coordinación de Seguridad e Infraestructura de la ANCP-CCE

La Coordinación de Seguridad e Infraestructura de la ANCP-CCE será responsable de liderar, implementar y mantener las estrategias, políticas y acciones necesarias para garantizar la seguridad de la información, la

ciberseguridad y la adecuada operación de la infraestructura tecnológica de la entidad. Sus responsabilidades incluyen:

1. Seguridad de la Información y Ciberseguridad

- Evaluar, identificar y estimar la brecha entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y la situación real de la entidad.
- Proyectar y actualizar los documentos técnicos de seguridad de la información (políticas, manuales, lineamientos).
- Promover y mantener una cultura de seguridad de la información entre los usuarios de los sistemas, archivos, datos e información.
- Realizar sensibilización y capacitación en seguridad de la información y digital.
- Conducir revisiones periódicas de seguridad y privacidad en la infraestructura y sistemas.
- Coordinar la gestión de incidentes de seguridad de la información y seguridad digital.
- Realizar análisis de vulnerabilidades y evaluar mejoras en plataformas tecnológicas.
- Solicitar aprobación de modificaciones a políticas y documentos ante el Comité Institucional de Gestión y Desempeño.

2. Infraestructura Tecnológica

- Implementar controles para garantizar la seguridad física y lógica de la infraestructura tecnológica.
- Administrar y gestionar el hardware de comunicaciones de red (LAN, WLAN, WAN) y asegurar su adecuada operación.
- Monitorear enlaces de telecomunicaciones, comportamiento de redes y servicios de internet.

- Establecer estándares, procedimientos y controles de administración y seguridad de componentes tecnológicos.
- Garantizar el funcionamiento de centros de datos locales o en la nube.
- Desarrollar e implementar estrategias de respaldo de información y configuración de infraestructura.
- Apoyar el despliegue de nuevas plataformas tecnológicas requeridas por la entidad.
- Establecer y monitorear niveles de acceso a datos, código fuente, equipos y sistemas.
- Monitorear y proyectar necesidades de ampliación de capacidad operativa del sistema de información.
- Proporcionar protección adecuada a documentos, datos y aplicaciones críticas.

3. Recuperación ante Desastres

- Realizar y/o supervisar pruebas a los planes de contingencia y recuperación ante desastres.
- Entregar informes con evidencias de las pruebas realizadas.
- Garantizar que el plan de recuperación este alineado con los estándares institucionales.

7.5. Responsabilidad del Asesor, Contratista u Oficial (o quién haga sus veces) designado para la Privacidad y la Protección de Datos Personales

- Informar, asesorar y emitir recomendaciones para la Protección de datos personales al área SIDT.
- Acompañar en el Trámite de las consultas y reclamos y derechos de los Titulares sobre protección de datos personales que sean remitidos a la SIDT.
- Apoyar el cumplimiento de las obligaciones para la protección de los datos personales que sean aplicables de acuerdo con la legislación

nacional vigente y aplicable (Documentos como Políticas, autorizaciones, avisos de privacidad, sensibilización y capacitación) de acuerdo con la autonomía de su posición.

- Coordinar y solicitar a nivel técnico con los líderes de los equipos de seguridad de la información, infraestructura interna y los administradores de los sistemas de la ANCP-CCE que se cumpla con las medidas de datos personales.
- Solicitar y apoyar a Identificar al área de riesgos de la entidad, los riesgos de cumplimiento en protección de datos personales.
- Trabajar con las áreas de seguridad e infraestructura tecnológica de forma conjunta, para la articulación de los incidentes de seguridad que estén asociados o tengan materialización de datos personales.
- Impulsar y participar en la elaboración del cronograma y plan de capacitación y sensibilización de protección de datos personales para la entidad y entrenamiento.
- Apoyar a la oficina jurídica para la creación o actualización de las cláusulas protección de datos personales y no divulgación de la información según sea el caso.

8. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El subsistema de Seguridad y Privacidad de la Información se encuentra alineado con la Política del Sistema Integrado de Gestión, en concordancia con el compromiso institucional de proteger la información institucional y personal. En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), se establecen roles, responsabilidades, controles técnicos y organizacionales, así como medidas específicas para la gestión de incidentes, continuidad del negocio, seguridad digital, uso de dispositivos, teletrabajo y respaldo de información.

Esta política, como parte integral del manual operativo, es de cumplimiento obligatorio para funcionarios, contratistas y terceros, y constituye el eje rector para la implementación de prácticas seguras en el tratamiento de la información.

Dentro de esta política se establecen los siguientes componentes de seguridad que tiene políticas específicas, lineamientos y procedimientos:

8.1. Componente de Política de Gobierno

8.1.1. Políticas para la seguridad de la información

Control Asociado en el MSPI A.5.1

Establecer una dirección y soporte para la seguridad de la información mediante políticas alineadas con los objetivos del negocio, Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Ante las necesidades de regulación en materia de seguridad y privacidad, considerando los riesgos identificados, requisitos legales y regulatorios, cambios tecnológicos, resultados de auditorías, incidentes de seguridad y necesidades de los procesos, se elaboran o actualizan las políticas y lineamientos de Seguridad de la Información correspondientes, definiendo su objetivo, alcance, responsabilidades, directrices de cumplimiento y mecanismos de seguimiento.
- Para realizar la revisión anual, el responsable debe verificar su vigencia frente a los cambios en la estructura y funcionamiento de la ANCP-CCE, tecnología, procesos, normatividad aplicable, riesgos de seguridad y privacidad, resultados de auditorías e incidentes de seguridad relevantes. Como resultado de la revisión, se debe determinar si el

documento se mantiene vigente, requiere actualización o debe ser reemplazado, dejando registro de la decisión adoptada.

- Una vez elaboradas o actualizadas, las políticas y lineamientos serán sometidos a revisión técnica y jurídica cuando corresponda y posteriormente presentados ante el COASIC y CIGD. La aprobación debe quedar soportada mediante el mecanismo formal definido por la ANCP-CCE, conservando como evidencia el acta, registro o documento de aprobación correspondiente.
- Cuando la revisión determine la necesidad de modificar una política o lineamiento, el responsable debe identificar los cambios realizados, actualizar la versión y fecha de vigencia, registrar los motivos de la modificación y gestionar nuevamente su aprobación antes de su publicación. Las versiones obsoletas deben retirarse de los medios de consulta general o conservarse en un repositorio histórico con acceso controlado, evitando que sean utilizadas como documentos vigentes.
- Una vez aprobadas, el responsable debe solicitar y coordinar su publicación a través de los canales institucionales oficiales definidos para tal fin. La publicación debe permitir su consulta por funcionarios, contratistas y terceros que tengan responsabilidades o actividades relacionadas con la seguridad y privacidad de la información. Cuando corresponda a información de carácter público, debe garantizarse su disponibilidad para consulta por parte de la ciudadanía, conforme a las disposiciones de transparencia y acceso a la información aplicables.
- Las políticas y lineamientos se mantendrán disponibles en medios institucionales oficiales, tales como intranet, sistema de gestión documental o repositorio institucional, asegurando que los usuarios consulten únicamente la versión vigente. Cada documento debe permitir identificar, como mínimo, su versión, fecha de aprobación, fecha de

vigencia, responsable y estado del documento.

- Además de la revisión anual, se debe iniciar una revisión cuando ocurran cambios significativos en la organización, procesos, tecnología o normatividad, se modifique el perfil de riesgos de seguridad y privacidad, se presenten incidentes relevantes, se identifiquen hallazgos de auditoría o se determine que las políticas existentes ya no responden adecuadamente a las necesidades de la ANCP-CCE.

8.1.2. Roles y responsabilidades de seguridad de la información

Control Asociado en el MSPI A.5.2

Definir los roles y la asignación de responsables para cada acción establecida dentro de la planeación de seguridad de la información como aspecto fundamental para el correcto funcionamiento del MSPI, Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- La asignación de responsabilidades de Seguridad de la Información se realizará durante la definición o actualización de los roles, procesos y estructuras organizacionales, tomando como referencia el Manual de Funciones, los procedimientos institucionales, la matriz RACI o de responsabilidades del SGSI/MSPI, la matriz de riesgos de seguridad de la información y los demás documentos normativos internos que resulten aplicables.
- El responsable del SGSI/MSPI, en coordinación con los líderes de proceso y responsables de las áreas, debe identificar las actividades de seguridad que requieren responsable, determinar el rol que tendrá a cargo su ejecución, establecer las autoridades necesarias para su cumplimiento y

definir los activos, información, sistemas o procesos bajo su responsabilidad. El detalle de los roles, autoridades y responsabilidades establecidos para el SGSI/MSPI se encuentra desarrollado en el Capítulo 7 – Roles y responsabilidades del presente Manual Operativo.

- Una vez asignadas o modificadas las responsabilidades, Seguridad de la Información coordinara su comunicación formal con los funcionarios, contratistas y terceros a quienes les sean aplicables.

- La comunicación se realizará mediante los mecanismos institucionales establecidos, tales como actas de asignación, comunicaciones oficiales, procesos de inducción o reinducción, capacitación, socialización de políticas y procedimientos, aceptación de obligaciones contractuales o mecanismos equivalentes, de acuerdo con la naturaleza del rol.

- Las responsabilidades de Seguridad de la Información se revisan como mínimo una vez al año y adicionalmente cuando se presenten cambios en la estructura organizacional, funciones de los cargos, procesos, tecnologías, sistemas de información, riesgos de seguridad, requisitos legales o controles del SGSI/MSPI.

- La verificación del cumplimiento se realiza mediante auditorías, revisiones periódicas, indicadores, controles establecidos, evidencias de ejecución, informes de gestión, seguimiento a incidentes y resultados de planes de mejoramiento, según corresponda a cada responsabilidad. Cuando se identifique un incumplimiento, Seguridad de la Información registra la situación, determinar su causa e impacto, define las acciones correctivas o de mejora necesarias, asigna responsables y fechas de cumplimiento y realiza el seguimiento hasta su cierre.

8.1.3. Segregación de funciones

Control Asociado en el MSPI A.5.3

Reducir el riesgo de errores o uso indebido mediante la separación de responsabilidades incompatibles. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Mediante la definición y mantenimiento de los roles, responsabilidades, niveles de autoridad y permisos de acceso requeridos para el desarrollo de las funciones institucionales, se gestiona el gobierno de identidades. Para ello, se identifican los recursos que requieren control de acceso, incluyendo instalaciones, áreas o dependencias seguras, sistemas de información, aplicaciones, bases de datos, infraestructura tecnológica y demás activos de información.

  La asignación de permisos se realiza con base en las funciones y responsabilidades formalmente asignadas al usuario, aplicando los principios de necesidad de conocer, mínimo privilegio y necesidad de uso. Antes de otorgar un acceso, se valida la autorización correspondiente y se verifica que el nivel de permiso solicitado sea consistente con las funciones del rol.

  La gestión de usuarios y permisos se gestionan mediante el Directorio Activo para gestionar el ciclo de vida de las identidades, dejando evidencia de la solicitud, autorización, ejecución y, cuando corresponda, revocación del acceso.

- La segregación de funciones se realiza mediante la identificación de actividades que, por su naturaleza, puedan generar conflictos de interés, fraude, uso indebido de privilegios, errores no detectados o concentración excesiva de autoridad.

- La información sobre segregación de funciones se revisa como mínimo una vez al año y adicionalmente cuando se presenten cambios en la estructura organizacional, procesos, funciones, sistemas de información, tecnologías, niveles de acceso o riesgos de seguridad.

- La efectividad de la segregación de funciones se valida mediante revisiones periódicas de la matriz de roles y responsabilidades y su contraste con los perfiles de acceso efectivamente asignados en los sistemas, aplicaciones e instalaciones correspondientes.

- Las funciones relacionadas con la solicitud, autorización, ejecución, administración y verificación de actividades críticas de seguridad de la información se asignan a personas o roles diferentes, evitando que una misma persona tenga control completo sobre un proceso. Se prioriza la segregación en actividades como:
  - Gestión de usuarios y privilegios.
  - Administración de sistemas e infraestructura.
  - Aprobación y ejecución de cambios.
  - Gestión de copias de respaldo y restauraciones.
  - Gestión de incidentes de seguridad.
  - Desarrollo, pruebas y puesta en producción.
  - Adquisición, contratación y supervisión de proveedores.
  - Administración y revisión de registros y logs.
  - Acceso a información clasificada o crítica.

Los dueños de los Sistemas:

- Las funciones y transacciones críticas de cada sistema de información se identifican y se establecen las combinaciones de roles incompatibles. Antes de asignar o modificar permisos, se valida que el perfil solicitado no permita a un mismo usuario ejecutar actividades que deben permanecer separadas. Las excepciones se justifican, autorizan y están sujetas a controles compensatorios y seguimiento. La segregación se verifica periódicamente mediante la revisión de perfiles y permisos, gestionando los conflictos identificados hasta su corrección o formalización como excepción.

Los jefes de las dependencias:

- Validar que el usuario no concentre funciones incompatibles que le permitan acceder, modificar, aprobar, ejecutar o utilizar activos de información sin la debida autorización o sin mecanismos de detección y supervisión. Estas validaciones se realizan con base en la matriz de roles y responsabilidades y en las reglas de segregación de funciones definidas por la ANCP-CCE.

- Cuando la segregación de funciones no sea técnica, operativa u organizacionalmente viable, se deben implementar controles compensatorios, entre otros:
- Revisión periódica de las actividades: verificar durante o después de la ejecución de las actividades críticas que estas se realicen de acuerdo con las autorizaciones, procedimientos y responsabilidades establecidas.
- Rastros de auditoría: mediante la revisión de registros, identificar quién realizó la actividad, qué acción ejecutó, sobre qué activo o información, cuándo la realizó y, cuando sea técnicamente posible, desde dónde se

efectuó. Los registros deben protegerse contra modificación o eliminación no autorizada y estar disponibles para las actividades de seguimiento e investigación.

- Supervisión de la gestión: mediante una revisión independiente por parte de un responsable diferente a quien ejecuta la actividad, especialmente para operaciones críticas o de alto riesgo. La supervisión debe quedar soportada mediante registros de revisión, aprobaciones, informes o evidencias equivalentes.

Los funcionarios y terceros de la entidad:

- los funcionarios y terceros de la entidad conocen sus funciones por medio de la matriz de roles y responsabilidades, los procesos y/o procedimientos y el manual de funciones, así como los lineamientos establecidos en este manual.

La ANCP-CCE sigue la siguiente matriz de segregación de funciones que permite identificar incompatibilidades entre roles y responsabilidades y establecer quién puede solicitar, aprobar, ejecutar y verificar cada actividad crítica

Tabla 1: matriz de segregación de funciones

Actividad	Solicita	Aprueba	Ejecuta	Verifica
Creación de usuario	Jefe/Responsable	Dueño del proceso	Administrador IAM/AD	Seguridad de la Información
Asignación de privilegios	Responsable del proceso	Dueño del activo	Administrador	Seguridad de la Información

Restauración de backup	Responsable del sistema	Dueño del proceso	Administrador Backup	Seguridad/TI
Cambio en producción	Responsable TI	Comité/Cambio autorizado	Administrador	Responsable del servicio
Acceso excepcional	Responsable del proceso	Responsable de Seguridad	Administrador	Auditoría/Seguridad

Fuente: elaboración propia

8.1.4. Gestión de responsabilidades

Control Asociado en el MSPI A.5.4

Asegurar que la dirección y supervisión estén comprometidas con la seguridad de la información. Este control esta alineado con la POLÍTICA DE ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. El detalle de los roles y responsabilidades está detallado en el capítulo 7 de este documento. Por lo tanto, se desarrollarán las siguientes actividades:

El COASIC y CIGD:

- Adopta el presente documento como parte integral del Modelo de Seguridad y Privacidad de la Información.
- Requiere a todos los funcionarios y terceros el cumplimiento normativo interno de la ANCP-CCE (políticas, directrices, lineamientos y procedimientos establecidos), así como la normatividad externa a la entidad relacionada con seguridad y privacidad de la información.
- Promueve el compromiso de todos los niveles de responsabilidad y autoridad de la ANCP-CCE en la implementación del Modelo de Seguridad y Privacidad de la Información.
- Verifica el cumplimento de las políticas de seguridad y privacidad de la

información y los objetivos definidos, alineados con las necesidades de la ANCP-CCE.

- Comunica la necesidad de definir y mantener una gestión de la seguridad y privacidad de la información representada por medio de los objetivos y las políticas de seguridad.
- Respalda y promueve a las personas para que contribuyan al desarrollo del Modelo de Seguridad y Privacidad de la Información y adquieran un rol de liderazgo en cada una de sus dependencias de responsabilidad.

Seguridad de la Información:

- Divulgar y capacitar a los funcionarios de la ANCP-CCE sobre las políticas, procedimientos y lineamientos de seguridad y privacidad de la información, mediante jornadas de inducción, reinducción, capacitación y sensibilización, utilizando los canales y medios institucionales definidos mediante el PIC. Estas actividades deben realizarse al ingreso del personal, ante cambios relevantes en los lineamientos y de acuerdo con el programa anual de capacitación. Se debe conservar como evidencia el material utilizado, registros de asistencia, evaluaciones y demás soportes de ejecución.
- Diseñar, implementar y mantener programas de capacitación, entrenamiento y educación en seguridad y privacidad de la información, mediante el análisis de las necesidades identificadas en la gestión de riesgos, resultados de auditorías, incidentes de seguridad, cambios tecnológicos, requisitos legales y obligaciones institucionales. Los programas deben establecer los temas, objetivos, población objetivo, responsables, cronograma, metodología y mecanismos de evaluación, dejando evidencia de su ejecución y de los resultados obtenidos.
- Establecer, implementar y mantener los lineamientos y políticas

requeridos para la operación del MSPI en la ANCP-CCE, mediante la identificación de requisitos legales, regulatorios, técnicos y organizacionales, el análisis de riesgos y la definición de controles y responsabilidades. Los documentos deben ser revisados y actualizados cuando se presenten cambios significativos en los procesos, riesgos, tecnologías o requisitos aplicables, sometidos a aprobación por la instancia competente y publicados a través de los medios institucionales autorizados. Se deben conservar las versiones aprobadas, registros de revisión, aprobación y publicación como evidencia.

- Coordinar con las dependencias la identificación y valoración de activos y riesgos de seguridad y privacidad de la información, mediante la identificación de activos, propietarios y responsables, clasificación de la información, identificación de amenazas y vulnerabilidades, valoración de probabilidad e impacto y determinación del nivel de riesgo inherente y residual, registrándola en CCE-GTI-FM-43 Matriz de activos de la información e índice de información reservada y clasificada. Con base en los resultados, se deben seleccionar y priorizar los controles y acciones de tratamiento correspondientes, asignando responsables, recursos y fechas de ejecución. Se deben conservar las matrices de riesgos, valoración de activos, planes de tratamiento y evidencias de seguimiento.
- Programar y verificar anualmente la actualización de los análisis de riesgos de seguridad y privacidad de la información de las dependencias, mediante la definición de un cronograma de revisión, solicitud de actualización de las matrices, validación de los resultados y seguimiento al cumplimiento de las actividades establecidas. La actualización debe realizarse adicionalmente cuando ocurran cambios significativos en procesos, activos, tecnologías, amenazas, vulnerabilidades, proveedores

o requisitos aplicables, o cuando se presenten incidentes que puedan modificar la valoración del riesgo. Se deben documentar los resultados y las acciones de tratamiento derivadas en la Matriz de riesgos.

- Implementar y operar mecanismos para identificar, registrar, monitorear y reportar eventos e incidentes de seguridad y privacidad de la información, mediante el uso de la herramienta FALCON, Azure Monitor y Oraclee Cloud Guard, canales formales de reporte, procedimientos de clasificación, priorización, escalamiento, atención y cierre. Los eventos e incidentes deben registrarse desde su identificación hasta su cierre, determinando responsables, acciones ejecutadas, tiempos de atención, evidencias y lecciones aprendidas, de acuerdo con su nivel de criticidad. Se deben conservar los registros y evidencias que permitan verificar su trazabilidad.
- Monitorear y verificar permanentemente el cumplimiento de las responsabilidades y lineamientos de seguridad y privacidad de la información, mediante la revisión de indicadores, controles, informes, registros, resultados de auditorías, evaluaciones de cumplimiento y evidencias proporcionadas por las dependencias responsables. Los incumplimientos deben ser registrados, comunicados a los responsables y gestionados mediante acciones correctivas o de mejora, estableciendo responsables, fechas de cumplimiento y mecanismos de seguimiento hasta su cierre y verificación de efectividad.
- Definir, implementar y mantener los procedimientos de continuidad operativa y recuperación ante desastres de la infraestructura tecnológica de la ANCP-CCE, mediante la identificación de servicios y activos críticos, análisis de dependencias, definición de RTO y RPO, establecimiento de estrategias de continuidad, procedimientos de contingencia, mecanismos de respaldo y recuperación y criterios para el retorno a la

operación normal. Para tal efecto existen los lineamientos de Copias de respaldo y restauración, Plan de pruebas de Recuperación y programa de pruebas de restauración. Los lineamientos deben probarse periódicamente mediante ejercicios y pruebas de recuperación, documentando los resultados, incumplimientos, tiempos obtenidos y acciones de mejora. Los lineamientos deben actualizarse cuando se presenten cambios relevantes en la infraestructura, servicios, riesgos o resultados de las pruebas.

Los jefes de las dependencias deben:

- Gestionar el cumplimiento de las políticas, lineamientos, directrices y procedimientos de seguridad y privacidad de la información por parte del personal bajo su responsabilidad, mediante su comunicación formal, inclusión en las actividades de inducción y reinducción (PIC), seguimiento periódico y verificación de la aplicación de los controles establecidos. Ante incumplimientos, deben definirse y realizarse las acciones correctivas o de mejora correspondientes. Como evidencia se deben conservar las comunicaciones, registros de capacitación, verificaciones realizadas y soportes de las acciones implementadas.
- Gestionar la activación, modificación, suspensión o desactivación de los accesos a la información digital clasificada como pública clasificada, pública reservada o datos personales no públicos, mediante los mecanismos de autorización y control de acceso establecidos por la ANCP-CCE. Las solicitudes deben estar justificadas, contar con la autorización del responsable correspondiente, establecer el período de vigencia cuando el acceso sea temporal y ser revisadas cuando cambien las funciones, responsabilidades o condiciones que originaron el acceso.

Se deben conservar las solicitudes, autorizaciones, registros de modificación y evidencias de activación o desactivación.

- Clasificar los activos de información bajo responsabilidad del proceso, mediante la identificación de sus requisitos de confidencialidad, integridad y disponibilidad, aplicando los criterios y metodología establecidos por la ANCP-CCE. La clasificación debe efectuarse durante el levantamiento o actualización del inventario de activos y revisarse cuando se presenten cambios en el activo, proceso, información, riesgos o requisitos aplicables. Se debe conservar el inventario actualizado, los criterios de valoración y los registros que soporten la clasificación realizada.
- Ejecutar, como mínimo una vez al año, el análisis y valoración de los riesgos de seguridad de la información de cada proceso, con el acompañamiento de Seguridad de la Información, mediante la identificación de activos, amenazas, vulnerabilidades, consecuencias, probabilidad e impacto, de acuerdo con la metodología y guía de gestión de riesgos establecida en el MANUAL METODOLÓGICO DE ADMIISTRACIÓN DE RIESGOS. El análisis debe actualizarse adicionalmente cuando se presenten cambios significativos en los procesos, activos, tecnologías, amenazas, vulnerabilidades, proveedores o requisitos aplicables, o cuando ocurra un incidente relevante. Los resultados deben utilizarse para determinar el nivel de exposición y confirmar o ajustar los requerimientos de confidencialidad, integridad y disponibilidad. Como evidencia se deben conservar las matrices de riesgos, valoraciones, actas o registros de revisión y planes de tratamiento derivados.
- Definir los requerimientos de seguridad y privacidad de la información aplicables a los activos bajo responsabilidad del proceso, con el

acompañamiento de Seguridad de la Información, mediante el análisis de la clasificación de la información, los resultados de la gestión de riesgos, requisitos legales y regulatorios, políticas institucionales, estándares aplicables y necesidades operativas del proceso. Los requerimientos deben establecerse antes de la implementación o adquisición de nuevos activos o servicios y revisarse cuando se presenten cambios que puedan afectar su nivel de protección. Se deben conservar como evidencia las especificaciones, requisitos de seguridad, conceptos técnicos, matrices de requerimientos y demás documentos que soporten las decisiones adoptadas.

- Solicitar a Seguridad de la Información las actividades de capacitación y sensibilización requeridas por la dependencia, mediante la identificación de las necesidades de formación derivadas de las funciones del personal, riesgos identificados, incidentes ocurridos, cambios normativos, tecnológicos o procedimentales y resultados de evaluaciones de conocimiento. Las solicitudes deben realizarse de acuerdo con el programa de capacitación establecido en el PIC o cuando se identifique una necesidad específica. Se deben conservar las solicitudes, contenidos, registros de asistencia, evaluaciones y demás evidencias de las actividades realizadas.
- Definir, documentar, implementar, mantener y actualizar los procedimientos asociados al proceso, incorporando en cada actividad los controles de seguridad y privacidad de la información aplicables, mediante la identificación de riesgos, responsabilidades, puntos de control, criterios de operación, mecanismos de verificación y evidencias requeridas. Los procedimientos deben revisarse periódicamente y actualizarse cuando se presenten cambios en procesos, tecnologías, riesgos, normativa, estructura organizacional o resultados de auditorías

e incidentes. Las versiones deben ser aprobadas, publicadas y controladas conforme al procedimiento de gestión documental de la ANCP-CCE.

- Realizar seguimiento al cumplimiento de las obligaciones de seguridad y privacidad de la información del proceso, mediante la revisión periódica de controles, indicadores, registros, informes, resultados de auditorías, compromisos y evidencias generadas por las actividades del proceso. Las desviaciones o incumplimientos deben registrarse, comunicarse a los responsables y gestionarse mediante acciones correctivas o de mejora, estableciendo responsables y fechas de cumplimiento. Se deben conservar los registros de seguimiento, resultados de las verificaciones y evidencias de cierre de las acciones.
- Reportar a Seguridad de la Información los eventos o incidentes asociados al incumplimiento de las responsabilidades de seguridad y privacidad de la información, utilizando los canales institucionales definidos (gestion_seguridad@colombiacompra.gov.co) y proporcionando, como mínimo, la información disponible sobre fecha y hora, activo o información afectada, descripción del evento, usuario o responsable involucrado, evidencias disponibles y acciones iniciales realizadas. El reporte debe efectuarse inmediatamente después de su identificación, de acuerdo con los tiempos y criterios establecidos en el procedimiento de gestión de incidentes. Se deben conservar los registros del reporte, evidencias aportadas, comunicaciones, acciones ejecutadas y demás soportes relacionados con su atención.
- Integrar la seguridad y privacidad de la información en las actividades y tareas de la dependencia, mediante la incorporación de controles y requisitos de seguridad en la planeación, ejecución, supervisión y cierre de las actividades del proceso, considerando la clasificación de la

información, los riesgos identificados y los controles definidos por el SGSI/MSPI. Esta integración debe verificarse durante la planificación de nuevas actividades, proyectos, adquisiciones, cambios tecnológicos o modificaciones de procesos. Como evidencia se deben conservar los planes de trabajo, procedimientos, listas de verificación, registros de control, actas y demás documentos que demuestren la aplicación de los requisitos de seguridad y privacidad.

8.1.5. Contacto con autoridades

Control Asociado en el MSPI A.5.5

Mantener contacto con las diferentes autoridades que puedan apoyar a solucionar incidentes de seguridad y privacidad de la información identificados en la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Identificar, documentar y mantener actualizados los procedimientos y protocolos para el contacto con las autoridades competentes en materia de seguridad y privacidad de la información, mediante la elaboración de un directorio institucional que incluya, como mínimo, autoridad, competencia, tipo de incidente que debe ser reportado, canal autorizado, datos de contacto, requisitos de reporte, tiempos de notificación y responsable interno de la comunicación. El directorio y los protocolos deben revisarse como mínimo anualmente y actualizarse cuando se modifiquen los datos de contacto, competencias, procedimientos de reporte o requisitos legales aplicables. Evidencia: procedimiento aprobado, directorio de autoridades, registros de revisión y actualización y soportes de las comunicaciones realizadas.
- Evaluar y gestionar los incidentes relacionados con la protección de

datos personales que puedan generar obligaciones de notificación ante la Superintendencia de Industria y Comercio (SIC), mediante la clasificación del incidente, determinación de la información y titulares afectados, análisis de las circunstancias y consecuencias, evaluación de los requisitos legales aplicables y coordinación con las áreas responsables de privacidad y jurídica. Cuando se determine la existencia de una obligación de reporte, la notificación debe realizarse dentro de los términos y utilizando los mecanismos establecidos por la autoridad competente. Evidencia: registro del incidente, análisis de impacto, concepto o decisión de reporte, comunicación presentada a la SIC, constancia de radicación y documentación asociada.

- Mantener habilitados y controlados los canales institucionales autorizados para contactar a las autoridades nacionales competentes, mediante la identificación de los medios oficiales de comunicación, responsables autorizados, mecanismos de autenticación cuando apliquen y procedimientos para el envío y recepción de información. Los canales deben utilizarse cuando la evaluación del incidente determine que existe una obligación legal, regulatoria, contractual o una necesidad de coordinación con una autoridad competente. La información suministrada debe ser validada previamente, limitarse a la información necesaria para la atención del incidente y conservarse de acuerdo con los requisitos de protección de datos, reserva y gestión documental. Evidencia: directorio de canales autorizados, registros de validación, comunicaciones, radicados, actas y soportes de coordinación.
- Evaluar los eventos e incidentes de seguridad y privacidad de la información que puedan requerir intervención de autoridades, mediante su clasificación, análisis de impacto sobre la confidencialidad, integridad y disponibilidad, identificación de obligaciones legales o regulatorias y

determinación de los criterios de escalamiento y reporte. Cuando el análisis determine la necesidad de intervención de una autoridad, debe gestionarse el reporte a través del canal oficial y dentro del plazo aplicable, dejando registro de la decisión y de las acciones adoptadas. Evidencia: registro y clasificación del incidente, análisis realizado, decisión de escalamiento, comunicaciones, radicados y seguimiento al caso.

- Mantener actualizada la relación institucional con las autoridades y organismos competentes en materia de seguridad y privacidad de la información, mediante la identificación periódica de las entidades relevantes, validación de sus datos de contacto, competencias, mecanismos de reporte y condiciones de atención. Esta relación debe revisarse como mínimo anualmente y cada vez que se presente un incidente que evidencie la necesidad de incorporar o actualizar una autoridad de contacto. Para efectos de coordinación podrán contemplarse, según la naturaleza del incidente y las competencias aplicables, entidades y organismos como el Centro Cibernético Policial (CCP), COLCERT, CSIRT-CCIT, Policía Nacional, Superintendencia de Industria y Comercio (SIC) y las autoridades competentes en materia de emergencias y desastres, entre otras. Evidencia: directorio actualizado de autoridades, registros de validación, comunicaciones institucionales y soportes de actualización.

8.1.6. Contacto con grupos de interés especiales

Control Asociado en el MSPI A.5.6

Establecer y mantener contactos apropiados con grupos de interés especial u otros, foros y asociaciones profesionales especializadas en seguridad y privacidad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Gestionar la participación activa del talento humano en grupos, asociaciones, comunidades y foros especializados en seguridad y privacidad de la información, mediante la identificación de comunidades de interés, evaluación de su pertinencia frente a las funciones y riesgos de la ANCP-CCE, gestión de las membresías y definición de los funcionarios que participarán en cada espacio. La participación debe priorizar temas relacionados con los riesgos, tecnologías, amenazas, controles y necesidades de conocimiento identificados por la entidad, y debe mantenerse mientras aporte valor al fortalecimiento de las competencias institucionales. Los funcionarios participantes deben compartir internamente los conocimientos, alertas, recomendaciones y buenas prácticas relevantes obtenidos en estos espacios. Evidencia: registro de membresías, listado de participantes, agenda o programación de actividades, constancias de participación y registros de socialización del conocimiento.
- Gestionar y mantener mecanismos de relacionamiento con universidades, grupos de investigación, proveedores de tecnología y demás organizaciones especializadas, mediante la identificación de entidades y fuentes confiables que generen boletines, alertas, publicaciones, investigaciones, contenidos de formación y actualizaciones relacionadas con seguridad y privacidad de la información. La información recibida debe ser revisada y clasificada periódicamente para determinar su pertinencia y, cuando resulte aplicable, ser difundida a los funcionarios responsables de seguridad y privacidad de la información o incorporada como insumo para la actualización de controles, procedimientos, análisis de riesgos y

programas de capacitación. Evidencia: directorio de entidades y fuentes de información, registros de contacto, boletines o publicaciones recibidas, análisis de pertinencia, comunicaciones de divulgación y registros de capacitación o socialización.

- Mantener mecanismos de comunicación y coordinación con grupos y comunidades especializadas en seguridad y privacidad de la información, mediante la participación en redes profesionales, comunidades de respuesta a incidentes, foros técnicos y otros espacios especializados que permitan consultar y compartir información sobre amenazas, vulnerabilidades, incidentes, medidas de contención y buenas prácticas. Ante la identificación de un incidente que pueda afectar la confidencialidad, integridad o disponibilidad de la información, se deben consultar las fuentes y comunidades especializadas que resulten pertinentes para obtener recomendaciones técnicas, validar estrategias de respuesta y, cuando corresponda, coordinar acciones de atención y recuperación. Evidencia: registros de membresía y participación, consultas realizadas, alertas recibidas, recomendaciones técnicas, comunicaciones, tickets de incidentes y documentación de las acciones adoptadas.

8.1.7. Seguridad de la información en la gestión de proyectos Control Asociado en el MSPI A.5.8

Integrar la seguridad de la información en la gestión de proyectos desde su planificación. Por lo tanto, se desarrollarán las siguientes actividades:

Proyectos o quien haga sus veces:

- Determinar la criticidad de la información que será utilizada, procesada,

almacenada o generada durante el proyecto, mediante la identificación de los activos de información involucrados y la aplicación de los criterios institucionales de clasificación, considerando sus requerimientos de confidencialidad, integridad y disponibilidad. Esta valoración debe realizarse durante la etapa de formulación o planificación del proyecto y actualizarse cuando se incorporen nuevos activos, se modifique el alcance o cambien las condiciones de tratamiento de la información. Evidencia: inventario de activos, matriz de clasificación, análisis de criticidad y registros de aprobación o validación.

- Definir las condiciones de uso, conservación, acceso y disposición de la información durante el ciclo de vida del proyecto, mediante el establecimiento del período de utilización, tiempo de conservación, criterios de archivo o eliminación y perfiles de acceso requeridos para funcionarios, contratistas y terceros. Los accesos deben asignarse bajo el principio de mínimo privilegio y mantenerse únicamente durante el período en que sean necesarios para cumplir las funciones asignadas. Estas condiciones deben revisarse ante cambios en el alcance, responsables, proveedores o requerimientos legales del proyecto. Evidencia: matriz de accesos, reglas de retención, autorizaciones, registros de asignación y revocación de accesos y soportes de disposición de la información.
- Incorporar los riesgos asociados a la privacidad y al tratamiento de datos personales en el análisis de riesgos previo a la ejecución del proyecto, mediante la identificación de los datos personales involucrados, finalidades y operaciones de tratamiento, titulares, responsables y encargados, amenazas, vulnerabilidades, impactos y requisitos legales aplicables. Los riesgos identificados deben valorarse y, cuando corresponda, establecerse medidas de tratamiento antes de la

aprobación o puesta en ejecución del proyecto. Evidencia: matriz de riesgos, análisis de privacidad, inventario de tratamientos, identificación de datos personales y plan de tratamiento.

- Formalizar los acuerdos de confidencialidad y las condiciones para la entrega, acceso, intercambio y devolución de información, mediante los instrumentos jurídicos y administrativos definidos por la ANCP-CCE y de conformidad con la normativa vigente. Los acuerdos deben gestionarse antes de proporcionar información confidencial, reservada o datos personales a funcionarios, contratistas o terceros que no cuenten previamente con las condiciones requeridas, y deben establecer como mínimo las obligaciones de uso, protección, custodia, divulgación, devolución o eliminación de la información. Evidencia: acuerdos de confidencialidad suscritos, actas de entrega, autorizaciones, registros de devolución o eliminación y demás documentos contractuales asociados.
- Aplicar prácticas de desarrollo seguro y ejecutar pruebas de seguridad en los proyectos que contemplen el desarrollo o modificación de sistemas de información, mediante la incorporación de requisitos de seguridad desde las etapas de análisis y diseño, revisión de código, gestión de vulnerabilidades, pruebas de seguridad, pruebas de penetración y corrección de las debilidades identificadas antes de la puesta en producción. La profundidad y alcance de las pruebas deben definirse de acuerdo con la criticidad, exposición, arquitectura y riesgos del sistema, y repetirse cuando existan cambios significativos o nuevas vulnerabilidades relevantes. Evidencia: requisitos de seguridad, resultados de revisiones de código, informes de análisis de vulnerabilidades y pruebas de penetración, registros de remediación y autorización para paso a producción.
- Identificar la participación de terceros en el proyecto y establecer

previamente los requisitos de seguridad, privacidad y confidencialidad que les sean aplicables, mediante la evaluación de las actividades que ejecutarán, la información y sistemas a los que tendrán acceso y los riesgos derivados de su participación. Antes de otorgar acceso o iniciar el tratamiento de información, deben formalizarse las cláusulas contractuales y autorizaciones correspondientes, incluyendo, cuando aplique, obligaciones de cumplimiento normativo, tratamiento de datos personales, confidencialidad, aceptación de las políticas de seguridad, requisitos de acceso, gestión de incidentes, devolución o eliminación de información y terminación de accesos. Evidencia: evaluación del tercero, contratos, anexos de seguridad, acuerdos de confidencialidad, autorizaciones de tratamiento, aceptación de políticas y registros de asignación y revocación de accesos.

- Evaluar, tratar y realizar seguimiento a los riesgos de seguridad de la información y privacidad asociados al proyecto durante todo su ciclo de vida, mediante revisiones formales al inicio, durante la ejecución y antes del cierre, así como ante cambios significativos en el alcance, tecnología, información tratada, proveedores, arquitectura, amenazas o requisitos aplicables. Los riesgos deben mantenerse registrados, con valoración actualizada, controles definidos, responsables, fechas de tratamiento y nivel de riesgo residual; las desviaciones deben gestionarse mediante acciones correctivas o de mejora y verificarse antes del cierre del proyecto. Evidencia: matriz de riesgos actualizada, actas de revisión, planes de tratamiento, informes de seguimiento, resultados de controles y acta o registro de cierre de riesgos.

Seguridad de la Información debe:

- Acompañar la gestión de los riesgos de seguridad de la información de

cada proyecto, mediante la identificación y valoración de activos, amenazas, vulnerabilidades e impactos, la definición de controles y acciones de tratamiento conforme a la metodología institucional y la revisión de los resultados durante las etapas de formulación, ejecución y cierre o cuando se presenten cambios significativos. Evidencia: matrices de riesgos, registros de acompañamiento, planes de tratamiento y soportes de seguimiento y cierre.

8.2. Componente Política de Administración de amenazas y vulnerabilidades

8.2.1. Inteligencia de amenazas

Control Asociado en el MSPI A.5.7

Recopilar y analizar la información relacionada con las amenazas a la seguridad y privacidad de la información de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Implementar mecanismos para anticipar, prevenir y reducir el impacto de las amenazas de seguridad de la información, mediante la recopilación y análisis oportuno de información sobre amenazas, vulnerabilidades, indicadores de compromiso, técnicas, tácticas y procedimientos utilizados por los actores de amenaza, y la definición de acciones preventivas, de detección, respuesta y mitigación. Los mecanismos deben activarse y ajustarse de acuerdo con el nivel de riesgo, la criticidad de los activos y la información obtenida del monitoreo y de fuentes de inteligencia. Evidencia: registros de análisis, alertas, recomendaciones, acciones preventivas y soportes de seguimiento.
- Implementar fuentes, herramientas y metodologías para identificar,

analizar y contextualizar las amenazas cibernéticas que puedan afectar a la ANCP-CCE, mediante el uso de fuentes internas y externas confiables, boletines de seguridad, organismos especializados, fabricantes, comunidades de ciberseguridad, reportes de vulnerabilidades, indicadores de compromiso y registros de eventos e incidentes de la entidad. La información debe recopilarse, validarse, correlacionarse y analizarse periódicamente y ante la identificación de amenazas relevantes, considerando su aplicabilidad a los activos, tecnologías, procesos y riesgos de la ANCP-CCE. Evidencia: inventario de fuentes, registros de consulta, reportes de inteligencia, análisis de amenazas, indicadores de compromiso y documentación de las fuentes utilizadas.

- Recopilar, validar, correlacionar y analizar la información relacionada con amenazas de seguridad de la información, mediante la revisión de fuentes internas y externas, comparación de información proveniente de diferentes fuentes, identificación de patrones, tendencias, indicadores de compromiso, técnicas y vulnerabilidades explotables y determinación de su posible afectación sobre los activos de la XXX. El análisis debe realizarse periódicamente y actualizarse cuando se identifiquen amenazas nuevas, cambios relevantes en el panorama de riesgo o incidentes que requieran análisis adicional. Evidencia: registros de recopilación, matrices de análisis, reportes técnicos, indicadores identificados y resultados de correlación.
- Elaborar, comunicar y socializar informes de inteligencia de amenazas, mediante la consolidación de los resultados del análisis, priorización de las amenazas según su relevancia, probabilidad e impacto y definición de recomendaciones dirigidas a las dependencias y responsables de los activos afectados. La información debe comunicarse utilizando canales

autorizados y aplicando controles que preserven su confidencialidad, integridad y disponibilidad, limitando el acceso de acuerdo con su clasificación. Los informes deben generarse con la periodicidad definida y adicionalmente cuando se identifiquen amenazas críticas o situaciones que requieran atención inmediata. Evidencia: informes emitidos, registros de distribución, actas de socialización, comunicaciones, recomendaciones y constancias de recepción.

- Implementar y hacer seguimiento a las acciones correctivas y preventivas derivadas de los análisis de inteligencia de amenazas, mediante la incorporación de las recomendaciones en los planes de tratamiento de riesgos, gestión de vulnerabilidades, configuración de controles, procedimientos de seguridad y demás mecanismos de tratamiento aplicables. Las acciones deben priorizarse de acuerdo con la criticidad de la amenaza, exposición de los activos y nivel de riesgo, asignando responsables y fechas de ejecución, y verificando posteriormente su efectividad. Evidencia: planes de tratamiento, tickets, registros de cambios, informes de remediación, evidencias de implementación y resultados de las verificaciones.
- Utilizar la inteligencia de amenazas como insumo para fortalecer los controles técnicos preventivos y de detección, mediante la incorporación de indicadores de compromiso, dominios, direcciones IP, hashes, patrones de comportamiento, reglas de detección y demás información relevante en las herramientas de seguridad disponibles, tales como firewalls, sistemas de detección y prevención de intrusiones, soluciones antimalware, EDR/XDR, SIEM y otros mecanismos de monitoreo. La información debe actualizarse de acuerdo con su vigencia y nivel de riesgo, verificando que las reglas o indicadores incorporados sean aplicables y no generen afectaciones indebidas a la operación. Evidencia:

registros de actualización de reglas, indicadores incorporados, configuraciones, alertas generadas, tickets y resultados de validación.

- Incorporar la inteligencia de amenazas como insumo para definir y ejecutar pruebas de seguridad y privacidad de la información, mediante la selección de escenarios, técnicas, vulnerabilidades y vectores de ataque que sean relevantes para el entorno tecnológico de la ANCP-CCE, de acuerdo con las amenazas identificadas. Los resultados de las pruebas deben compararse con el panorama de amenazas vigente y utilizarse para identificar debilidades, ajustar controles y definir acciones de tratamiento. Las pruebas deben realizarse de acuerdo con el programa institucional y adicionalmente cuando se identifiquen amenazas que puedan afectar activos críticos. Evidencia: planes y casos de prueba, resultados de pruebas, informes de vulnerabilidades, evidencias de remediación y registros de validación.
- Compartir información de inteligencia de amenazas con otras entidades y comunidades especializadas, mediante canales institucionales autorizados y mecanismos de intercambio seguro de información, priorizando información que contribuya a la prevención, detección y respuesta frente a amenazas comunes. Antes de compartir información debe verificarse su clasificación, autorización, nivel de sensibilidad y cumplimiento de las restricciones legales, contractuales y de protección de datos aplicables. El intercambio debe realizarse cuando aporte valor a la gestión de riesgos, respuesta a incidentes o fortalecimiento de las capacidades de ciberseguridad. Evidencia: registros de intercambio, comunicaciones, acuerdos de colaboración, información compartida y soportes de autorización.
-

8.2.2. Gestión de vulnerabilidades técnicas

Control Asociado en el MSPI A.5.8

Obtener oportunamente la información relacionada con las vulnerabilidades técnicas de los sistemas de información utilizados en la entidad, evaluar la exposición a estas vulnerabilidades y tomar las medidas requeridas para tratar los riesgos que se pueden asociar. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Programar y ejecutar pruebas de análisis de vulnerabilidades sobre una muestra representativa de los sistemas de la ANCP-CCE, mediante herramientas y metodologías técnicamente reconocidas, considerando la criticidad de los activos, nivel de exposición, tecnologías utilizadas, antecedentes de vulnerabilidades y resultados de ejercicios anteriores. Las pruebas deben programarse como mínimo una vez al año en el cronograma anual de seguridad y ejecutarse adicionalmente cuando se presenten cambios significativos en los sistemas, nuevas vulnerabilidades críticas, incidentes de seguridad o condiciones que incrementen el nivel de exposición. El alcance de las pruebas debe definirse de acuerdo con los recursos técnicos, humanos y financieros asignados, priorizando los activos críticos y expuestos. Evidencia: cronograma anual, alcance aprobado, registros de ejecución, herramientas utilizadas e informes de resultados.
- Definir y mantener indicadores para monitorear la identificación, gestión y remediación de vulnerabilidades técnicas, mediante métricas que permitan medir, entre otros aspectos, número y severidad de vulnerabilidades identificadas, porcentaje de vulnerabilidades remediadas dentro del plazo establecido, tiempo promedio de

remediación, vulnerabilidades críticas y altas pendientes, activos evaluados y nivel de exposición. Los indicadores deben revisarse periódicamente y utilizarse como insumo para priorizar actividades, asignar recursos y tomar decisiones sobre tratamiento y aceptación del riesgo. Evidencia: fichas técnicas de indicadores, tableros de seguimiento, informes periódicos y registros de las decisiones adoptadas.

- Mantener actualizado el inventario de sistemas y activos tecnológicos sometidos a análisis de vulnerabilidades, mediante el registro de cada activo evaluado, identificación del responsable, fecha y tipo de análisis realizado, alcance, herramienta utilizada, resultado general y estado de las acciones de remediación. El inventario debe actualizarse después de cada análisis y cuando se incorporen, retiren, modifiquen o cambien de criticidad los sistemas o activos tecnológicos. Evidencia: inventario actualizado, registros de análisis, historial de evaluaciones y soportes de actualización.
- Presentar a la SIDT los resultados de los análisis de vulnerabilidades realizados, mediante informes que consoliden las vulnerabilidades identificadas, su severidad, activos afectados, nivel de exposición, evidencia técnica, recomendaciones de remediación y prioridad de atención. A partir de los resultados, deben definirse y programarse las actividades de corrección, mitigación o tratamiento, asignando responsables y fechas de ejecución de acuerdo con la criticidad de las vulnerabilidades. Evidencia: informes de vulnerabilidades, actas o registros de presentación, cronograma de remediación, tickets y planes de acción.
- Definir, aprobar e implementar controles compensatorios o mitigatorios cuando una vulnerabilidad no pueda ser remediada dentro del plazo

requerido, mediante el análisis de las causas que impiden la corrección, valoración del riesgo residual, identificación de medidas alternativas y evaluación de su efectividad. La aceptación del riesgo residual debe ser realizada por el responsable con la autoridad definida en la metodología institucional, estableciendo responsable, plazo de vigencia, controles implementados, fecha de revisión y condiciones que obliguen a reevaluar la decisión. El plan de acción debe ser objeto de seguimiento periódico hasta la remediación de la vulnerabilidad o el cierre formal del riesgo. Evidencia: análisis de riesgo residual, autorización de aceptación del riesgo, controles compensatorios implementados, plan de acción, registros de seguimiento y evidencias de cierre.

- Solicitar y verificar a los proveedores de sistemas de información las evidencias de los análisis de vulnerabilidades realizados sobre los sistemas e infraestructura bajo su responsabilidad, mediante la incorporación de este requisito en los contratos, acuerdos de nivel de servicio o demás instrumentos aplicables y mediante la solicitud periódica de informes técnicos, resultados de pruebas y evidencias de remediación. La documentación debe ser revisada para verificar como mínimo el alcance de las pruebas, fecha de ejecución, metodología utilizada, vulnerabilidades identificadas, nivel de severidad y estado de tratamiento. Cuando se identifiquen vulnerabilidades críticas o altas sin tratamiento adecuado, deben solicitarse las acciones de remediación correspondientes y realizar seguimiento hasta su cierre o aceptación formal del riesgo. Evidencia: solicitudes realizadas, informes de vulnerabilidades de los proveedores, conceptos de revisión, compromisos de remediación, evidencias de corrección y registros de seguimiento.

La SIDT debe:

- Aplicar los requisitos establecidos en las políticas, normas y lineamientos de seguridad de la información de la ANCP-CCE en los sistemas de información bajo responsabilidad de la dependencia, mediante la incorporación de controles de seguridad durante su implementación, configuración, operación, mantenimiento y actualización. Su cumplimiento debe verificarse durante las revisiones técnicas, cambios relevantes, análisis de vulnerabilidades y evaluaciones de seguridad. Evidencia: configuraciones, listas de verificación, informes de revisión, registros de cambios y demás soportes que demuestren la aplicación de los controles.
- Mantener disponibles las herramientas, licencias, servicios y contratos de soporte requeridos para actualizar y mantener las plataformas tecnológicas, mediante la identificación de las necesidades de soporte, renovación o actualización, la programación de los mantenimientos y la verificación de la vigencia de los servicios contratados. La disponibilidad de estos mecanismos debe revisarse periódicamente y antes de ejecutar actualizaciones críticas o cuando el fabricante publique nuevas versiones, parches o alertas de seguridad. Evidencia: contratos, licencias, órdenes de servicio, vigencias de soporte, registros de actualización y documentación técnica.
- Elaborar y gestionar el cronograma de remediación de las vulnerabilidades identificadas en la infraestructura tecnológica, mediante la priorización de las vulnerabilidades según su criticidad, exposición, impacto sobre los activos y riesgo asociado, definiendo actividades, responsables, fechas objetivo y dependencias requeridas. El cronograma debe presentarse a Seguridad de la Información para su

seguimiento y debe actualizarse cuando cambien las condiciones técnicas o de riesgo. Una vez implementadas las acciones, Seguridad de la Información debe verificar la corrección mediante actividades de re-test, de acuerdo con la disponibilidad de recursos y la criticidad de las vulnerabilidades. Evidencia: cronograma, plan de remediación, tickets, registros de cambio, evidencias de corrección e informes de re-test.

- Implementar los controles compensatorios o mitigatorios definidos y aprobados por Seguridad de la Información cuando una vulnerabilidad no pueda ser remediada de manera inmediata, mediante la aplicación de medidas técnicas, administrativas o procedimentales que reduzcan la probabilidad de explotación o el impacto sobre el activo afectado. La efectividad de los controles debe verificarse periódicamente y mantenerse mientras permanezca la condición que impide la remediación. Evidencia: aprobación del control, configuración implementada, registros de cambio, evidencias de funcionamiento y resultados de las verificaciones.
- Mantener los servicios tecnológicos en versiones soportadas y seguras, mediante el seguimiento de los ciclos de vida definidos por los fabricantes, revisión de boletines de seguridad y evaluación de nuevas versiones, actualizaciones y parches disponibles. Las actualizaciones deben priorizarse según la criticidad del servicio, nivel de exposición y severidad de las vulnerabilidades corregidas, evitando mantener versiones fuera de soporte sin una justificación y tratamiento formal del riesgo. Evidencia: inventario de versiones, registros de ciclo de vida, boletines de fabricantes, planes de actualización, registros de cambio y evidencias de actualización.
- Ejecutar pruebas técnicas y funcionales antes de implementar nuevas versiones de software, firmware o actualizaciones de seguridad en

ambientes productivos, mediante ambientes de prueba o mecanismos controlados que permitan validar compatibilidad, estabilidad, funcionamiento de las aplicaciones, integridad de la información y controles de seguridad. Las pruebas deben realizarse antes de cambios que puedan afectar la disponibilidad o funcionalidad de los servicios, y los resultados deben ser evaluados antes de autorizar el paso a producción. Evidencia: planes y resultados de pruebas, casos de prueba, actas o registros de aprobación, evidencias de respaldo y autorizaciones de cambio.

- Aplicar las actualizaciones de seguridad y mantenimiento requeridas sobre la infraestructura tecnológica, mediante la gestión formal de cambios, considerando los resultados de las pruebas, ventanas de mantenimiento, respaldos, procedimientos de reversión y criterios de validación posteriores a la implementación. Las actualizaciones deben ejecutarse cuando sean necesarias para garantizar la operación, corregir vulnerabilidades o atender alertas emitidas por Seguridad de la Información, fabricantes u organismos especializados, priorizando aquellas clasificadas como críticas o de alto riesgo. Evidencia: solicitudes y autorizaciones de cambio, registros de ejecución, respaldos, bitácoras, resultados de validación y documentación de reversión cuando aplique.
- Realizar análisis periódicos de seguridad sobre los sistemas de información, mediante herramientas automatizadas y técnicas de evaluación que permitan identificar vulnerabilidades, configuraciones inseguras, desviaciones frente a los estándares y demás condiciones que puedan afectar la seguridad de los servicios. Los resultados deben analizarse, clasificarse y documentarse en informes técnicos que permitan determinar las acciones de tratamiento requeridas. Evidencia: resultados de herramientas, informes técnicos, matrices de hallazgos,

planes de tratamiento y registros de seguimiento.

- Ejecutar revisiones técnicas de seguridad durante las actividades de análisis, diseño, desarrollo, implementación y mantenimiento de las aplicaciones, mediante la aplicación de listas de verificación, revisión de requisitos de seguridad, análisis de código cuando corresponda, evaluación de configuraciones y demás controles definidos para el desarrollo seguro. Las revisiones deben realizarse antes de la puesta en producción y ante cambios significativos en las aplicaciones. Evidencia: listas de verificación, resultados de revisiones, informes técnicos, registros de vulnerabilidades y autorizaciones para paso a producción.
- Gestionar los incumplimientos identificados durante las revisiones técnicas de seguridad, mediante el registro del hallazgo, análisis de su causa, valoración del riesgo, definición de acciones correctivas y asignación de responsables y fechas de ejecución. Las acciones deben ser objeto de seguimiento hasta su implementación y posterior verificación de efectividad. Evidencia: registros de hallazgos, análisis de causa, planes de acción, evidencias de implementación y resultados de las verificaciones.
- Reportar a Seguridad de la Información los eventos e incidentes asociados con pérdida, daño, robo o compromiso de activos de información derivados de vulnerabilidades o fallas de seguridad, mediante los canales institucionales establecidos para la gestión de incidentes, proporcionando la información disponible sobre el activo afectado, vulnerabilidad identificada, fecha y hora, impacto, acciones realizadas y evidencias disponibles. El reporte debe efectuarse inmediatamente después de su identificación y de acuerdo con los tiempos establecidos en el procedimiento de gestión de incidentes. Evidencia: tickets, registros de incidentes, comunicaciones, evidencias

técnicas y soportes de las acciones ejecutadas.

- Desarrollos internos y subcontratados
- Mantener disponibles las herramientas, licencias y contratos de soporte requeridos para actualizar y corregir los desarrollos de software subcontratados, mediante la incorporación de requisitos de mantenimiento, actualización, soporte, gestión de vulnerabilidades y atención de incidentes en los contratos y acuerdos de nivel de servicio. La vigencia y cumplimiento de estas condiciones debe verificarse durante la ejecución contractual y antes de requerir actualizaciones o remediaciones al proveedor. Evidencia: contratos, acuerdos de nivel de servicio, licencias, solicitudes de soporte, reportes del proveedor y registros de actualización.
- Elaborar y gestionar el cronograma de remediación de las vulnerabilidades identificadas en desarrollos internos o subcontratados, mediante la clasificación de los hallazgos según criticidad, exposición y riesgo, la definición de actividades de corrección, responsables, fechas objetivo y criterios de validación. El cronograma debe ser presentado a Seguridad de la Información para seguimiento y actualizado cuando se modifique el nivel de riesgo o las condiciones técnicas. Una vez implementadas las correcciones, debe realizarse el correspondiente re-test para verificar la eliminación o mitigación de las vulnerabilidades. Evidencia: informes de vulnerabilidades, cronograma, tickets, evidencias de corrección, informes de re-test y registros de cierre.
- Reportar a Seguridad de la Información los eventos e incidentes relacionados con la pérdida, daño, robo o compromiso de desarrollos internos o subcontratados derivados de vulnerabilidades, mediante los canales definidos para la gestión de incidentes y proporcionando la información técnica disponible para facilitar su análisis, contención y

tratamiento. El reporte debe realizarse inmediatamente después de su identificación y debe mantenerse la trazabilidad de las acciones ejecutadas hasta el cierre del incidente. Evidencia: registro del incidente, comunicaciones, análisis técnico, evidencias de contención y recuperación, acciones de remediación y registro de cierre.

8.3. Componente Política de Administración de activos

8.3.1. Inventario de información y otros activos asociados Control Asociado en el MSPI A.5.9

Identificar y gestionar los activos de información para asegurar su protección adecuada. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Ejercer el gobierno sobre los activos de información identificados por las dependencias de la entidad, mediante la definición, implementación y aplicación de procedimientos, circulares, lineamientos y demás instrumentos que establezcan las condiciones para su identificación, recolección, administración, aseguramiento de la calidad, consistencia, depuración y uso, coordinando las actividades con las dependencias responsables y dentro del ámbito de sus competencias. Estas actividades deben ejecutarse durante el ciclo de vida de los activos y revisarse cuando se presenten cambios en los procesos, sistemas, responsables, requisitos legales o condiciones de uso de la información. Evidencia: procedimientos, circulares y lineamientos aprobados, inventarios de activos, registros de actualización, matrices de responsables, reportes de calidad o depuración de datos y actas o registros de coordinación.
- Definir y mantener actualizados los criterios para la identificación de los activos de información, mediante la aplicación conjunta de criterios de

identificación, alcance, propietario o responsable, ubicación, proceso asociado, tipo de información, dependencia responsable y demás atributos establecidos en la metodología institucional de gestión de activos. Los criterios deben revisarse periódicamente y actualizarse cuando se modifique la metodología, el modelo MSPI, los procesos institucionales o las características de los activos. Evidencia: metodología o lineamientos de identificación, criterios documentados, formatos de inventario, matrices de activos, registros de revisión y actualizaciones realizadas.

Seguridad de la Información:

- Capacitar y acompañar a las dependencias en la gestión de los activos de información, mediante jornadas de inducción, capacitación, asesorías y acompañamiento técnico sobre identificación, registro, clasificación, valoración, actualización y tratamiento de los activos. Las actividades deben ejecutarse durante la implementación de la metodología, ante cambios relevantes en los lineamientos y como mínimo de acuerdo con el programa anual de capacitación. Evidencia: plan y material de capacitación, registros de asistencia, evaluaciones, solicitudes de acompañamiento, actas y demás soportes de asesoría.
- Realizar seguimiento a la gestión de los activos de información, mediante la revisión periódica del cumplimiento de los lineamientos establecidos en los numerales 5.10, 5.12, 5.13 y 5.14, verificando como mínimo la identificación, clasificación, etiquetado, manejo y demás controles aplicables a los activos. El seguimiento debe realizarse de acuerdo con el cronograma institucional y adicionalmente cuando se identifiquen cambios, incumplimientos o situaciones que puedan afectar la seguridad de la información. Evidencia: listas de verificación, informes de

seguimiento, matrices de cumplimiento, registros de hallazgos, planes de acción y evidencias de cierre.

- Solicitar y verificar la actualización periódica del inventario de activos de información, mediante la comunicación formal a las dependencias responsables para que revisen y validen la existencia, vigencia, responsable, ubicación, clasificación y estado de cada activo, registrando las novedades relacionadas con la creación, modificación, traslado, cambio de responsable o eliminación. La actualización debe realizarse con la periodicidad definida en la metodología y adicionalmente cuando se presenten cambios significativos en los procesos, sistemas o información. Evidencia: solicitudes de actualización, inventarios validados, registros de cambios, actas de revisión y soportes de creación, modificación o eliminación de activos.
- Definir, implementar y mantener actualizada la metodología para la gestión de activos de información, mediante la integración de los requisitos relacionados con protección de datos personales, el Manual para la Protección de Datos Personales, los lineamientos de MinTIC, ISO/IEC 27001, los procedimientos de gestión y retención documental y demás requisitos legales y reglamentarios aplicables. La metodología debe revisarse periódicamente y actualizarse ante cambios normativos, modificaciones de los lineamientos de MinTIC, cambios en los procesos institucionales o resultados de evaluaciones y auditorías. Evidencia: metodología aprobada, matriz de requisitos, versiones controladas, registros de revisión, actualizaciones normativas y documentos de aprobación.

Los jefes de las dependencias:

- Ejercer control sobre los activos de información bajo responsabilidad de la dependencia, mediante la identificación, registro, clasificación, valoración, asignación de responsables y actualización de la información registrada en el inventario institucional. El control debe mantenerse durante todo el ciclo de vida del activo y revisarse cuando se presenten cambios en su responsable, ubicación, proceso asociado, clasificación, criticidad o condición de uso. Evidencia: inventario actualizado, registros de activos, responsables asignados, matrices de clasificación y valoración y registros de cambios.
- Gestionar los activos de información a través del funcionario designado como enlace de Seguridad de la Información de la dependencia, mediante la coordinación de las actividades de identificación, registro, clasificación, actualización y validación de los activos, así como la comunicación de novedades y requerimientos con Seguridad de la Información. Las actividades deben realizarse de manera permanente y ante cualquier cambio que afecte los activos de la dependencia. Evidencia: designación formal del enlace, comunicaciones, registros de gestión, inventarios actualizados, actas y soportes de coordinación.
- Incluir los activos de información de la dependencia en los programas y actividades de seguridad y privacidad de la información, mediante su incorporación en las actividades de gestión de riesgos, análisis de vulnerabilidades, clasificación de información, capacitación, monitoreo, auditorías, continuidad y demás programas definidos en el SGSI/MSPI, de acuerdo con su criticidad y nivel de riesgo. La inclusión debe verificarse durante la planeación de cada programa y actualizarse cuando se incorporen, modifiquen o eliminen activos. Evidencia:

matrices de participación, planes y programas, inventarios, matrices de riesgos, registros de actividades, informes y resultados de seguimiento.

- Incorporar en el inventario de activos de información los parámetros aplicables de las Tablas de Retención Documental de la ANCP-CCE, mediante la asociación de los activos documentales y de información con las series, subseries, tiempos de retención, disposición final y demás criterios documentales que correspondan. Esta información debe verificarse durante la identificación y actualización de los activos y cuando se modifiquen las disposiciones de gestión documental aplicables. Evidencia: inventario de activos, Tablas de Retención Documental aplicables, registros de asociación documental y soportes de validación.
- Revisar y actualizar el inventario de activos de información, mediante la validación de la existencia, estado, responsable, ubicación, clasificación, valoración y demás atributos definidos en la metodología institucional. La revisión debe realizarse como mínimo una vez al año y adicionalmente cuando existan disposiciones internas, requerimientos de Seguridad de la Información, cambios significativos en los procesos, incorporación o eliminación de activos o modificaciones en las condiciones de operación. Evidencia: inventario actualizado y validado, registros de revisión, solicitudes de actualización, control de cambios y actas o comunicaciones de validación.
- Aprobar las actualizaciones realizadas sobre los activos de información de la dependencia, mediante la revisión de los cambios registrados en el inventario y la validación de que estos correspondan a modificaciones reales en los activos, sus responsables, ubicación, clasificación, valoración, estado o características. La aprobación debe efectuarse antes de considerar formalmente actualizado el inventario y cada vez que se

registren modificaciones que requieran aprobación. Evidencia: registros de aprobación, actas, comunicaciones, flujos de aprobación de la herramienta y versiones controladas del inventario.

- Aprobar los activos de información de la dependencia una vez finalizado su proceso de identificación, registro, clasificación y valoración, mediante la revisión de la información diligenciada y la confirmación de que los campos y criterios definidos en la metodología institucional se encuentren completos, consistentes y soportados. La aprobación debe realizarse antes de incorporar el activo como registro definitivo del inventario institucional y ante cada actualización integral del inventario. Evidencia: inventario aprobado, registros de validación, aprobación en la herramienta, actas o comunicaciones de aprobación.
- Diligenciar y mantener completos los campos definidos en la metodología institucional para la gestión de activos de información, mediante el registro de la información requerida para cada activo, incluyendo como mínimo su identificación, tipo, responsable, ubicación, proceso asociado, clasificación, valoración, requisitos aplicables y demás atributos establecidos por Seguridad de la Información. La información debe validarse antes de aprobar el activo y actualizarse cuando cambien sus características o condiciones de operación. Evidencia: registros completos en la herramienta institucional, inventarios, matrices de clasificación y valoración y reportes de validación.

8.3.2. Uso aceptable de la información y otros activos

Control Asociado en el MSPI A.5.10

Identificar, documentar e implementar reglas para el uso aceptable de la información y otros activos asociados con información e instalaciones de

procesamiento de información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Establecer y mantener los lineamientos para el uso aceptable de los activos de información, mediante la elaboración, aprobación y publicación de circulares, instructivos, procedimientos o documentos equivalentes que definan las condiciones de uso, restricciones, responsabilidades y conductas permitidas para los usuarios internos y terceros. Estos documentos deben revisarse periódicamente y actualizarse cuando se presenten cambios normativos, tecnológicos, organizacionales o de riesgo. Evidencia: política, procedimiento, circular o instructivo aprobado, control de versiones, registros de publicación y soportes de revisión.
- Capacitar a los funcionarios y terceros sobre el uso seguro y adecuado de los activos de información, mediante jornadas de inducción, reinducción, capacitación y sensibilización que incluyan los requisitos de seguridad y privacidad aplicables a la protección, acceso, tratamiento, almacenamiento, intercambio y disposición de la información. La capacitación debe realizarse durante la vinculación, ante cambios relevantes en los requisitos y de acuerdo con el programa anual de formación. Evidencia: plan de capacitación, contenidos, registros de asistencia, evaluaciones y evidencias de divulgación.
- Divulgar y mantener disponibles los lineamientos de uso aceptable de los activos de información, mediante los canales institucionales autorizados y mecanismos que permitan acreditar su comunicación a funcionarios y terceros. La divulgación debe realizarse al momento de la vinculación, ante modificaciones de los lineamientos y periódicamente

de acuerdo con el programa de sensibilización. Evidencia: publicaciones, comunicaciones, registros de envío, constancias de conocimiento, material de sensibilización y control de versiones.

- Incorporar los riesgos asociados al uso aceptable de los activos de información en la metodología de gestión de riesgos de seguridad de la información, mediante la identificación de amenazas, vulnerabilidades, eventos de riesgo, impactos sobre la confidencialidad, integridad y disponibilidad y controles aplicables. La evaluación debe realizarse durante los ejercicios de análisis de riesgos y actualizarse cuando se presenten cambios significativos, incidentes o nuevas condiciones de uso. Evidencia: matrices de riesgos, análisis de riesgos, planes de tratamiento, registros de actualización y seguimiento.
- Definir controles para prevenir y restringir el acceso no autorizado a los activos de información, mediante la aplicación de controles de autenticación, autorización, gestión de privilegios, segregación de funciones, monitoreo y trazabilidad, de acuerdo con la clasificación, criticidad y riesgo de cada activo. Los controles deben revisarse periódicamente y ajustarse cuando cambien los riesgos, tecnologías, usuarios o condiciones de acceso. Evidencia: matrices de acceso, configuraciones, registros de autorización, logs, informes de monitoreo y resultados de revisiones.

SIDT:

- Implementar medidas de seguridad para el uso de entornos de trabajo colaborativos, mediante la configuración de controles de autenticación, autorización, permisos de acceso, compartición de información, protección de datos, registro de actividades y administración de usuarios. Estas medidas deben aplicarse antes de habilitar nuevos

servicios colaborativos y revisarse cuando se modifiquen las plataformas, configuraciones o riesgos asociados. Evidencia: configuraciones de seguridad, matrices de permisos, registros de usuarios, políticas de compartición, logs y resultados de revisiones.

- Implementar y verificar los controles de restricción de acceso no autorizado definidos por Seguridad de la Información, mediante mecanismos técnicos de autenticación, autorización, control de privilegios, segmentación, monitoreo y registro de eventos. Los controles deben monitorearse periódicamente y adicionalmente cuando se presenten incidentes, cambios significativos o alertas de seguridad, verificando que funcionen conforme a los criterios establecidos. Evidencia: configuraciones, registros de acceso, logs, reportes de monitoreo, resultados de pruebas y registros de acciones correctivas.
- Proteger las copias temporales o permanentes de la información de los activos, mediante mecanismos técnicos que controlen su acceso, almacenamiento, transmisión, cifrado, retención y eliminación, de acuerdo con la clasificación y los requisitos de seguridad aplicables. Los mecanismos deben mantenerse durante todo el periodo en que existan las copias y revisarse cuando cambien las condiciones de almacenamiento o tratamiento. Evidencia: configuraciones de seguridad, controles de acceso, registros de almacenamiento, mecanismos de cifrado, políticas de retención y evidencias de eliminación.
- Mantener los activos de hardware y software en condiciones seguras y soportadas, mediante la aplicación de las recomendaciones técnicas de los fabricantes, gestión de actualizaciones y parches, mantenimiento preventivo y correctivo, control de versiones y seguimiento del ciclo de vida tecnológico. Las actividades deben ejecutarse de acuerdo con los

cronogramas de mantenimiento y ante la publicación de actualizaciones o alertas críticas de seguridad. Evidencia: inventarios, registros de versiones, contratos de soporte, boletines de fabricantes, órdenes de mantenimiento, registros de actualización y evidencias de configuración.

Compras y Contratos:

- Incorporar obligaciones de confidencialidad y protección de los activos de información en los contratos con terceros, mediante acuerdos de confidencialidad, cláusulas contractuales, anexos de seguridad y demás instrumentos que establezcan las condiciones para el acceso, uso, tratamiento, almacenamiento, intercambio, devolución y eliminación de información, incluyendo aquella procesada mediante servicios de computación en la nube pública. Estos requisitos deben verificarse antes de otorgar acceso o iniciar el tratamiento de información por parte del tercero. Evidencia: contratos, acuerdos de confidencialidad, anexos de seguridad, autorizaciones y registros de cumplimiento.
- Incorporar en los instrumentos contractuales las responsabilidades y consecuencias aplicables al uso indebido de los activos de información, mediante cláusulas que establezcan las obligaciones del proveedor o tercero frente a la protección de la información, incumplimientos, daños, incidentes y demás responsabilidades civiles, administrativas o penales que resulten aplicables conforme al marco jurídico vigente. Estas condiciones deben verificarse durante la revisión jurídica y técnica previa a la formalización del contrato. Evidencia: contratos, cláusulas de seguridad, conceptos jurídicos, listas de verificación y actas de revisión contractual.

Jefes de las dependencias:

- Supervisar el uso aceptable de los activos de información bajo responsabilidad de la dependencia, mediante la aplicación de los controles definidos según su clasificación y requisitos de confidencialidad, integridad y disponibilidad. La supervisión debe realizarse durante la operación de los procesos y ante cambios en los activos, usuarios o condiciones de acceso. Evidencia: inventarios, matrices de acceso, registros de supervisión, reportes de incidentes y resultados de verificaciones.
- Aplicar los requisitos de seguridad de la información establecidos para la protección de la información, los activos asociados y los recursos utilizados para su tratamiento, mediante el cumplimiento de las políticas, procedimientos, controles técnicos y administrativos definidos por la entidad. Su cumplimiento debe verificarse durante las actividades de supervisión, auditoría, gestión de riesgos y atención de incidentes. Evidencia: listas de verificación, informes de auditoría, registros de cumplimiento, evidencias de configuración y reportes de incidentes.
- Gestionar, procesar y almacenar la información de acuerdo con su clasificación, mediante la aplicación de los controles establecidos para cada nivel de clasificación, incluyendo restricciones de acceso, mecanismos de almacenamiento, transmisión, intercambio, copia y eliminación. Estas condiciones deben aplicarse durante todo el ciclo de vida de la información y revisarse cuando cambie su clasificación o nivel de riesgo. Evidencia: inventario y clasificación de activos, matrices de acceso, configuraciones, registros de transferencia y evidencias de disposición.
- Utilizar los mecanismos institucionales definidos para proteger las copias temporales o permanentes de la información, mediante el uso de

repositorios, plataformas, mecanismos de respaldo, cifrado, controles de acceso y demás soluciones autorizadas por la SIDT. El cumplimiento debe verificarse durante las revisiones de seguridad y cuando se detecten copias almacenadas en ubicaciones no autorizadas. Evidencia: registros de almacenamiento, configuraciones, respaldos, permisos de acceso, reportes de monitoreo y registros de eliminación.

- Formalizar los acuerdos de confidencialidad antes de intercambiar o entregar información a terceros, mediante el diligenciamiento, revisión y suscripción de los formatos institucionales correspondientes, verificando que incluyan las obligaciones de protección, uso permitido, restricciones de divulgación, devolución o eliminación de la información. El acuerdo debe formalizarse antes de efectuar la entrega o habilitar el acceso, salvo las excepciones legalmente establecidas. Evidencia: acuerdos de confidencialidad suscritos, autorizaciones, registros de entrega o acceso y soportes de devolución o eliminación.

Funcionarios y terceros:

- Utilizar las instalaciones y recursos destinados al procesamiento de información de acuerdo con los lineamientos institucionales de seguridad, mediante el cumplimiento de las políticas, procedimientos, controles de acceso, restricciones de uso, medidas de protección física y lógica y demás condiciones establecidas para las instalaciones y recursos tecnológicos. El cumplimiento debe verificarse mediante los mecanismos de monitoreo, supervisión y gestión de incidentes definidos por la entidad y ante cualquier incumplimiento identificado. Evidencia: registros de acceso físico y lógico, logs, reportes de monitoreo, actas de supervisión, registros de capacitación y reportes de incidentes.

8.3.3. Devolución de activos

Control Asociado en el MSPI A.5.11

Garantizar la devolución oportuna de activos al finalizar una relación laboral o contractual. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Establecer y aplicar procedimientos para la entrega y recepción de bienes y activos físicos de la entidad, mediante formatos o registros que permitan identificar el activo, responsable, estado, fecha de entrega, fecha de devolución y novedades identificadas. El procedimiento debe aplicarse al inicio, modificación y terminación de la relación laboral o contractual, así como ante cambios de dependencia o reasignación de activos. Evidencia: procedimiento aprobado, actas de entrega y devolución, formatos de inventario, registros de asignación y soportes de novedades.

SIDT

- Establecer y aplicar lineamientos para la entrega, asignación y devolución de los activos de información y recursos tecnológicos, mediante mecanismos que permitan registrar y controlar datos, equipos de cómputo, hardware, software, medios de almacenamiento y demás recursos tecnológicos entregados a funcionarios y terceros. Los lineamientos deben aplicarse durante la asignación, reasignación y devolución de los activos y actualizarse cuando cambien las tecnologías, procesos o requisitos de seguridad. Evidencia: lineamientos aprobados, formatos de entrega y devolución, inventarios, registros de asignación y actas de recepción.
- Identificar y mantener documentados los activos de información y

recursos tecnológicos que deben ser devueltos al finalizar o suspender una vinculación, mediante inventarios asociados al usuario, cargo, contrato o dependencia y listas de verificación de retiro que permitan identificar, como mínimo, equipos especializados, mecanismos de autenticación físicos, copias físicas de información, equipos de cómputo, dispositivos de almacenamiento, software, licencias y demás elementos asignados. La identificación debe revisarse al momento de la notificación de terminación, cambio de dependencia o suspensión temporal de actividades. Evidencia: inventarios individuales, listas de verificación de retiro, registros de asignación, actas de devolución y constancias de validación.

- Controlar la realización de copias no autorizadas de información durante el período de notificación de terminación o cesación temporal de actividades, mediante la aplicación de restricciones sobre puertos USB, dispositivos de almacenamiento, servicios de transferencia, correo electrónico, herramientas de colaboración y demás mecanismos definidos según el nivel de riesgo del usuario y de la información. Los controles deben mantenerse durante el período definido por la entidad y retirarse o modificarse únicamente cuando corresponda, verificando su aplicación mediante registros de monitoreo. Evidencia: configuraciones de seguridad, políticas de restricción, registros de eventos, alertas, reportes de monitoreo y evidencias de retiro o modificación de controles.

Funcionarios y terceros

- Devolver los activos de información y demás recursos asignados o generados durante la relación laboral o contractual, mediante la entrega física o transferencia controlada de documentos, datos, equipos de

cómputo, hardware, software, medios de almacenamiento, credenciales, dispositivos y demás elementos suministrados o generados por la entidad. La devolución debe realizarse antes de la finalización efectiva del vínculo o actividad, y adicionalmente cuando se produzca un cambio de dependencia o reasignación de funciones. Evidencia: acta o formato de devolución, inventario actualizado, registros de transferencia, constancia de recepción y reporte de novedades.

- Transferir la información institucional que haya sido creada, recibida, modificada o reproducida durante el desarrollo de las funciones, mediante los repositorios, sistemas de información o mecanismos institucionales autorizados, verificando que la información quede disponible para el responsable designado y que se mantenga su integridad, clasificación y trazabilidad. La transferencia debe realizarse antes de finalizar la relación laboral o contractual, o inmediatamente cuando sea requerida por el responsable de la dependencia. Evidencia: registros de transferencia, actas de entrega, ubicación del repositorio institucional, confirmación del responsable receptor y registros de acceso.
- Eliminar de forma segura las copias de información institucional almacenadas en los equipos o medios utilizados por el funcionario o tercero, mediante los mecanismos de borrado seguro definidos por la SIDT, una vez realizada y validada la transferencia de la información y cuando la conservación de dichas copias no sea necesaria ni esté autorizada. La eliminación debe ejecutarse antes de la devolución del equipo o finalización del vínculo, preservando las evidencias requeridas cuando existan obligaciones legales, contractuales o de investigación. Evidencia: registros de borrado seguro, certificados o actas de eliminación, evidencias técnicas, listas de verificación de retiro y

constancias de validación.

8.4. Componente Política de Protección de Información

8.4.1. Clasificación de la información

Control Asociado en el MSPI A.5.12

Identificar y clasificar los activos de información de acuerdo con su criticidad teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información y requisitos legales. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Definir y mantener actualizados los criterios y niveles de clasificación de la información, mediante una metodología que permita valorar los activos de información de acuerdo con su criticidad y los requisitos de confidencialidad, integridad y disponibilidad (CIA), estableciendo los niveles, reglas de valoración y condiciones de aplicación para cada tipo de información. Los criterios deben revisarse periódicamente y actualizarse ante cambios normativos, metodológicos, organizacionales o tecnológicos. Evidencia: metodología de clasificación, matriz de criterios y niveles, registros de valoración, versiones aprobadas y evidencias de revisión.
- Comunicar los procedimientos y guías para la clasificación de la información y gestión del inventario de activos, mediante los canales institucionales definidos, acompañados de instructivos, capacitaciones o sesiones de orientación que expliquen la identificación, creación, clasificación, valoración y actualización de los activos. La comunicación debe realizarse durante la implementación de la metodología, ante modificaciones y como parte de las actividades periódicas de sensibilización. Evidencia: procedimientos y guías publicadas,

comunicaciones, registros de capacitación, material divulgado y constancias de socialización.

- Disponer y mantener habilitada una herramienta para la clasificación y valoración de los activos de información, mediante una solución institucional que permita a los propietarios registrar, clasificar, valorar, actualizar y consultar la información de sus activos conforme a los criterios definidos en la metodología. La herramienta debe mantenerse disponible y sus funcionalidades deben revisarse cuando se modifique la metodología o los requerimientos de gestión. Evidencia: herramienta habilitada, registros de activos, clasificaciones y valoraciones realizadas, perfiles de acceso y reportes de gestión.
- Definir los controles de seguridad aplicables a la información compartida con terceras partes, mediante la determinación de requisitos de acceso, confidencialidad, integridad, disponibilidad, protección de datos, transferencia, almacenamiento, conservación, devolución y eliminación, de acuerdo con la clasificación de la información y el nivel de riesgo asociado. Los controles deben establecerse antes de autorizar el intercambio y revisarse cuando cambien las condiciones de la relación o el riesgo. Evidencia: lineamientos de intercambio, matrices de controles, requisitos de seguridad, acuerdos de confidencialidad, anexos contractuales y registros de aprobación.

Jefes de las dependencias:

- Clasificar y valorar la información bajo responsabilidad de la dependencia, mediante la aplicación de los criterios, niveles, procedimientos y herramientas definidos por Seguridad de la Información, considerando como mínimo su impacto sobre la confidencialidad, integridad y disponibilidad. La clasificación debe

realizarse durante la creación o incorporación del activo al inventario y actualizarse cuando cambien sus características, uso, criticidad, requisitos legales o nivel de riesgo. Responsable: jefe de la dependencia, con participación de los propietarios de los activos y apoyo del enlace de Seguridad de la Información. Evidencia: inventario de activos, registros de clasificación y valoración, matrices CIA y aprobaciones correspondientes.

- Aprobar la entrega o suministro de información a personas naturales o jurídicas externas, mediante la verificación previa de la clasificación de la información, finalidad de la entrega, autorización del propietario, requisitos legales, necesidad de acceso y controles de protección aplicables. La aprobación debe obtenerse antes de realizar la entrega o habilitar el acceso, salvo las excepciones establecidas legalmente. Evidencia: solicitud y autorización de entrega, acuerdos de confidencialidad, registros de transferencia, permisos de acceso y constancias de recepción.
- Revisar periódicamente la clasificación y valoración de los activos de información, mediante la validación de los niveles asignados, cambios en la criticidad, condiciones de tratamiento, amenazas, vulnerabilidades y requisitos legales aplicables. La revisión debe realizarse como mínimo una vez al año y adicionalmente ante cambios significativos, incidentes, modificaciones de procesos, nuevos riesgos o requerimientos de Seguridad de la Información. Evidencia: registros de revisión, inventarios actualizados, matrices de valoración, cambios de clasificación, informes y actas de validación.
- Controlar los períodos de almacenamiento y conservación de la información física y electrónica, mediante la aplicación de los tiempos y disposiciones establecidos en las Tablas de Retención Documental y

demás requisitos legales o institucionales aplicables, verificando periódicamente que la información que haya cumplido su período de conservación sea identificada para su disposición final. La eliminación debe ejecutarse mediante mecanismos seguros y autorizados, preservando las evidencias requeridas cuando existan obligaciones legales, contractuales o de investigación. Evidencia: Tablas de Retención Documental, inventarios, registros de disposición final, actas de eliminación, certificados de destrucción y evidencias de borrado seguro.

SIDT:

- Implementar y mantener los controles técnicos definidos para proteger los datos y la información compartida con terceras partes, mediante mecanismos de autenticación, autorización, cifrado, control de acceso, transferencia segura, registro de actividades, monitoreo y demás medidas establecidas según la clasificación y riesgo de la información. Los controles deben verificarse periódica y adicionalmente ante cambios en los servicios, terceros, configuraciones o condiciones de riesgo. Evidencia: configuraciones de seguridad, matrices de acceso, certificados o parámetros de cifrado, registros de transferencia, logs, reportes de monitoreo y resultados de pruebas.

Custodios de los activos de información:

- Aplicar los controles de protección definidos para los activos de información bajo su custodia, mediante la implementación de las medidas técnicas, físicas y administrativas correspondientes al nivel de clasificación asignado, incluyendo controles de acceso, almacenamiento, transmisión, copia, conservación y disposición. Los controles deben mantenerse durante todo el período de custodia y verificarse ante

cambios en la clasificación, condiciones de tratamiento o instrucciones del propietario. Evidencia: registros de acceso, configuraciones, controles implementados, bitácoras, registros de almacenamiento, transferencia y disposición.

- Notificar a los propietarios de los activos las situaciones que puedan representar riesgos para la información bajo custodia, mediante los canales institucionales establecidos para el reporte de eventos e incidentes, proporcionando información sobre el activo afectado, situación identificada, fecha, impacto potencial, acciones realizadas y evidencias disponibles. La notificación debe efectuarse inmediatamente después de identificar la condición de riesgo y mantenerse hasta su atención o escalamiento correspondiente. Evidencia: reportes o tickets, registros de incidentes, comunicaciones, evidencias técnicas, acciones de contención y registros de seguimiento.

8.4.2. Etiquetado de la información

Control Asociado en el MSPI A.5.13

Establecer procedimientos y/o lineamientos para el etiquetado de la información, de acuerdo con el esquema de clasificación adoptado por la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Definir y mantener actualizado el procedimiento para el etiquetado de la información, mediante la determinación de reglas, formatos, niveles, ubicación, contenido mínimo y mecanismos de aplicación asociados a cada nivel del esquema de clasificación adoptado por la entidad. El procedimiento debe revisarse periódicamente y actualizarse cuando se modifique el esquema de clasificación, la normativa aplicable, las

tecnologías utilizadas o los riesgos identificados. Evidencia: procedimiento aprobado, matriz de clasificación y etiquetado, formatos o ejemplos de etiquetas, control de versiones y registros de revisión.

- Divulgar el procedimiento de etiquetado de la información a funcionarios y terceros, mediante capacitaciones, inducciones, reinducciones, comunicaciones y publicación en los canales institucionales definidos. La divulgación debe realizarse durante la vinculación, ante modificaciones del procedimiento y de acuerdo con el programa institucional de sensibilización. Evidencia: material de capacitación, registros de asistencia, comunicaciones, publicaciones y constancias de divulgación.
- Sensibilizar y reforzar la aplicación del procedimiento de etiquetado de la información, mediante campañas, ejemplos prácticos, instructivos y actividades de seguimiento que permitan a los usuarios identificar cuándo y cómo aplicar las etiquetas según la clasificación de la información. Estas actividades deben realizarse periódicamente y reforzarse cuando se identifiquen errores, incumplimientos o cambios en los criterios de clasificación. Evidencia: campañas, piezas de sensibilización, instructivos, registros de capacitación, resultados de verificaciones y reportes de incumplimiento.
- Incorporar los documentos de ofimática dentro del esquema institucional de etiquetado, mediante la definición y configuración de mecanismos que permitan aplicar la clasificación y etiqueta correspondiente a documentos de texto, hojas de cálculo, presentaciones y demás formatos utilizados por la entidad. La aplicación debe efectuarse durante la creación, modificación o distribución de documentos sujetos a clasificación. Evidencia: configuración de las herramientas, plantillas, documentos etiquetados, pruebas de funcionamiento y registros de validación.

- Utilizar la clasificación de los activos de información como criterio para determinar su etiquetado, mediante la correspondencia entre los niveles de clasificación definidos en el inventario de activos y las etiquetas aplicables a la información contenida o asociada a cada activo. Esta correspondencia debe verificarse durante la clasificación inicial y cada vez que se modifique la valoración o clasificación del activo. Evidencia: matriz de correspondencia clasificación-etiquetado, inventario de activos, registros de clasificación y resultados de validación.

SIDT:

- Implementar y mantener los mecanismos tecnológicos para aplicar el etiquetado de la información, mediante la configuración de las herramientas institucionales que permitan asignar, visualizar, conservar y, cuando corresponda, hacer cumplir las etiquetas de acuerdo con los procedimientos y niveles de clasificación definidos por Seguridad de la Información. Los mecanismos deben probarse antes de su puesta en operación y revisarse ante cambios tecnológicos, actualizaciones o modificaciones del esquema de clasificación. Evidencia: configuraciones, políticas de etiquetado, registros de pruebas, documentación técnica, reportes de funcionamiento y evidencias de actualización.
- Jefes de las dependencias
- Verificar que los activos de información de la dependencia se encuentren etiquetados de acuerdo con su clasificación, mediante la revisión del inventario de activos, una muestra de la información generada y los registros de etiquetado disponibles en las herramientas institucionales. La verificación debe realizarse periódicamente, como mínimo durante la revisión anual del inventario, y cuando se creen, modifiquen o reclasifiquen activos. Evidencia: listas de verificación, inventarios,

muestras de información etiquetada, registros de revisión y acciones correctivas.

- Aplicar etiquetas de información reconocibles y de fácil interpretación, mediante el uso exclusivo de las etiquetas, formatos, nomenclaturas y mecanismos definidos institucionalmente para cada nivel de clasificación, evitando etiquetas ambiguas, duplicadas o que puedan generar confusión durante el acceso, manejo, intercambio o almacenamiento de la información. La aplicación debe verificarse durante la creación y actualización de la información y en las revisiones de cumplimiento. Evidencia: documentos y activos etiquetados, formatos institucionales, listas de verificación y resultados de las revisiones.
- Validar el etiquetado de la información asociada a los activos registrados en la matriz de activos de la dependencia, mediante la comparación entre la clasificación registrada en el inventario y las etiquetas aplicadas a la información física y electrónica asociada. La validación debe efectuarse durante la actualización del inventario y cuando se modifique la clasificación de un activo. Evidencia: matriz de activos, registros de clasificación, resultados de validación, muestras revisadas y registros de corrección.

Funcionarios y terceros:

- Aplicar el etiquetado a la información que generen, reciban, modifiquen o administren, mediante los criterios establecidos en el MSPI, la clasificación institucional, las Tablas de Retención Documental (TRD) tanto soportes físicos como electrónicos. El etiquetado debe realizarse desde la creación o recepción de la información y mantenerse durante su ciclo de vida, actualizándose cuando cambie su clasificación o

condición de acceso. Evidencia: documentos físicos y electrónicos etiquetados, registros del sistema, inventarios, formatos institucionales y soportes de clasificación.

- Etiquetar la información conforme al procedimiento institucional y a su nivel de clasificación, mediante la selección de la etiqueta correspondiente y su aplicación en los documentos, archivos, medios físicos o electrónicos y demás soportes que contengan información clasificada. Antes de compartir, transferir, almacenar o disponer la información, el usuario debe verificar que la etiqueta corresponda con su clasificación y con las condiciones autorizadas de manejo. Responsable: funcionarios y terceros. Evidencia: documentos y archivos etiquetados, registros de transferencia, controles de acceso, evidencias de almacenamiento y resultados de verificaciones.

8.4.3. Transferencia de información

Control Asociado en el MSPI A.5.14

Proteger la información en tránsito contra accesos no autorizados, modificaciones o pérdidas. Por lo tanto, se desarrollarán las siguientes actividades:

SIDT:

- Mantener actualizado el inventario de la información electrónica compartida con terceros y otras entidades, mediante un registro que identifique como mínimo la información objeto de intercambio, activo de origen, propietario, destinatario, finalidad, medio de transferencia, clasificación, fecha, vigencia de la autorización y condiciones de acceso. Antes de efectuar cualquier transferencia o intercambio, debe verificarse la existencia del requerimiento y la autorización del propietario del

activo. Evidencia: inventario de información compartida, solicitudes, autorizaciones, registros de transferencia y trazabilidad de las operaciones.

- Implementar controles de seguridad para proteger la transmisión, transferencia e intercambio de información, mediante cifrado, autenticación, control de acceso, canales seguros, validación de destinatarios, protección contra malware, integridad de archivos y mecanismos de trazabilidad, de acuerdo con la clasificación y riesgo de la información. Los controles deben aplicarse antes de cada intercambio y verificarse periódicamente o ante cambios en las tecnologías, canales o riesgos identificados. Evidencia: configuraciones de seguridad, certificados o parámetros de cifrado, políticas de transferencia, registros de acceso, logs y resultados de pruebas.
- Activar y enviar a la plataforma institucional de análisis de eventos los registros de actividad asociados a los servicios utilizados para transferir información, mediante la configuración de los mecanismos de generación, recolección, transmisión, almacenamiento y correlación de logs. La cobertura debe verificarse durante la incorporación de nuevos servicios y mediante revisiones periódicas que permitan confirmar la recepción y disponibilidad de los registros. Evidencia: configuraciones de logging, registros recibidos, reglas de correlación, reportes de monitoreo y evidencias de revisión.
- Mantener actualizado el inventario de conexiones utilizadas por terceros y de los usuarios e información a los que tienen acceso, mediante el registro del tercero, conexión, usuario, activo, permisos, finalidad, vigencia y responsable de autorización. El inventario debe revisarse periódicamente y actualizarse inmediatamente ante altas, modificaciones o terminaciones de accesos. Evidencia: inventario de

conexiones, matrices de acceso, autorizaciones, registros de altas y bajas y reportes de revisión.

- Utilizar mecanismos seguros para la transferencia e intercambio de información mediante medios físicos, mediante el empleo de medios autorizados, cifrado cuando corresponda, controles de acceso, embalaje seguro, identificación del destinatario y mecanismos de trazabilidad y cadena de custodia. Estas medidas deben aplicarse antes de cada transferencia y de acuerdo con la clasificación de la información y el tipo de medio utilizado. Evidencia: registros de transferencia, cadena de custodia, actas de entrega y recepción, controles de cifrado y registros de autorización.
- Aplicar prácticas y controles reconocidos para la protección del intercambio de información, mediante la adopción de estándares técnicos, controles de seguridad institucionales, recomendaciones de fabricantes y prácticas reconocidas de ciberseguridad, seleccionadas de acuerdo con el riesgo, clasificación y tecnología utilizada. La pertinencia de estos controles debe revisarse periódicamente y ante cambios tecnológicos o de riesgo. Evidencia: estándares adoptados, procedimientos, configuraciones, evaluaciones técnicas y registros de revisión.
- Restringir el uso de herramientas colaborativas web para el intercambio de información clasificada, mediante configuraciones técnicas que permitan limitar la carga, compartición o transferencia de información a los niveles autorizados. Como regla general, la información compartida mediante estas herramientas debe corresponder a información clasificada como pública, salvo autorización expresa y aplicación de controles adicionales definidos según el riesgo. Evidencia: configuraciones de restricciones, políticas de uso, registros de

compartición, autorizaciones y reportes de monitoreo.

- Proporcionar y mantener habilitados canales seguros para el intercambio de información con entidades y terceros autorizados, mediante plataformas institucionales que incorporen autenticación, autorización, cifrado, control de acceso, trazabilidad y mecanismos de protección de la información, previa existencia de un acuerdo o instrumento formal que establezca las condiciones del intercambio. Adicionalmente, deben implementarse controles para supervisar el envío de información mediante correo electrónico hacia dominios externos. Evidencia: acuerdos suscritos, configuraciones de plataformas, matrices de acceso, registros de transferencia, políticas de correo y reportes de monitoreo.
- Implementar mecanismos de etiquetado para identificar información sensible o crítica durante su transferencia, mediante el uso de las etiquetas definidas en el esquema institucional de clasificación y los mecanismos tecnológicos disponibles para conservar dicha identificación durante el intercambio. La aplicación debe verificarse antes de efectuar transferencias que involucren información sensible o crítica. Evidencia: etiquetas aplicadas, configuraciones, documentos transferidos, registros de transferencia y resultados de validación.

Seguridad de la Información

- Definir y verificar medidas de seguridad para los canales de comunicación contratados con terceros, mediante requisitos de autenticación, cifrado, control de acceso, gestión de vulnerabilidades, monitoreo, registro de eventos y respuesta ante incidentes, determinados según la clasificación de la información y el riesgo del servicio. Los requisitos deben establecerse antes de la entrada en operación del canal y revisarse periódicamente o ante cambios en el

servicio o proveedor. Evidencia: requisitos de seguridad, anexos técnicos, evaluaciones de riesgo, contratos, configuraciones y reportes de monitoreo.

- Incorporar compromisos de seguridad para el intercambio de información en los acuerdos internacionales, mediante la definición de obligaciones sobre confidencialidad, integridad, disponibilidad, protección de datos, canales autorizados, restricciones de uso, incidentes, conservación, devolución y eliminación de la información, de acuerdo con la legislación y acuerdos aplicables. Los compromisos deben establecerse antes del intercambio y revisarse cuando cambien las condiciones del acuerdo. Evidencia: acuerdos internacionales, cláusulas de seguridad, conceptos jurídicos, autorizaciones y registros de revisión.
- Divulgar los lineamientos para la transferencia e intercambio seguro de información física, electrónica y verbal, mediante capacitaciones, campañas, instructivos y comunicaciones que establezcan los controles aplicables según la clasificación de la información y el medio utilizado. La divulgación debe realizarse durante la vinculación, ante cambios relevantes y de acuerdo con el programa institucional de sensibilización. Evidencia: material de capacitación, registros de asistencia, comunicaciones, campañas y evaluaciones.

Jefes de las dependencias que entregan información a terceros

- Aplicar los requisitos establecidos en la Política de Protección de Datos Personales para el intercambio, transmisión o transferencia de información que contenga datos personales, mediante la verificación de la finalidad, autorización, base legal, destinatario, condiciones de tratamiento, medidas de seguridad y responsabilidades de las partes antes de realizar el intercambio. La verificación debe efectuarse antes

de cada nuevo intercambio y cuando cambien la finalidad, información, destinatario o condiciones de tratamiento. Evidencia: autorizaciones, análisis de tratamiento, acuerdos de transmisión o transferencia, registros de entrega y soportes de cumplimiento.

- Formalizar los acuerdos para el intercambio de información con entidades externas, mediante convenios, acuerdos de intercambio, acuerdos de confidencialidad, anexos de seguridad u otros instrumentos jurídicos que definan como mínimo la finalidad, información objeto de intercambio, responsabilidades, controles de seguridad, restricciones de uso, protección de datos, gestión de incidentes y condiciones de devolución o eliminación. El acuerdo debe formalizarse antes de efectuar el intercambio, salvo las excepciones legalmente establecidas. Evidencia: convenios, acuerdos suscritos, anexos de seguridad, autorizaciones y registros de intercambio.
- Reportar los incidentes que afecten la información intercambiada, transmitida o transferida, mediante los canales institucionales establecidos para la gestión de incidentes, suministrando información sobre el activo afectado, tercero involucrado, tipo de información, fecha y hora, situación identificada, impacto y evidencias disponibles. El reporte debe realizarse inmediatamente después de su identificación y mantenerse actualizado hasta su cierre. Evidencia: ticket o registro del incidente, comunicaciones, evidencias técnicas, acciones de contención, seguimiento y cierre.
- Autorizar la extracción de información de las bases de datos corporativas, mediante la solicitud formal del responsable del proceso o propietario del activo, indicando finalidad, información requerida, destinatario, alcance, clasificación, medio de extracción y condiciones de protección. La autorización debe obtenerse antes de ejecutar la

extracción y debe conservarse la trazabilidad de la información extraída. Evidencia: solicitud y autorización de extracción, registros de consulta o extracción, archivos generados, logs y registros de entrega.

Gestión Administrativa

- Controlar la transferencia de información mediante medios físicos de almacenamiento, mediante procedimientos que regulen la preparación, identificación, embalaje, autorización, entrega, transporte, recepción y devolución de documentos, archivos, carpetas, discos, cintas y demás medios. Los controles deben aplicarse antes y durante cada transferencia, de acuerdo con la clasificación de la información. Evidencia: formatos de entrega y recepción, registros de transferencia, inventarios y cadenas de custodia.
- Verificar el correcto direccionamiento y recepción de la información física y electrónica, mediante la validación previa de destinatarios, direcciones, cuentas, números de contacto y autorizaciones, manteniendo registros que permitan reconstruir el recorrido de la información y acreditar su recepción. La validación debe realizarse antes de cada envío y durante la recepción cuando corresponda. Evidencia: guías de envío, registros de entrega, confirmaciones de recepción, cadenas de custodia y trazabilidad electrónica.
- Prevenir el envío de información al destinatario equivocado, mediante mecanismos de doble verificación del destinatario, dirección, cuenta de correo, número telefónico y contenido antes de efectuar el envío. Para información clasificada como sensible, reservada o crítica debe aplicarse una validación adicional o mecanismo de aprobación definido institucionalmente. Evidencia: listas de verificación, registros de aprobación, confirmaciones de destinatario y trazabilidad del envío.

- Impedir el reenvío automático del correo institucional hacia cuentas externas, mediante la aplicación de políticas y configuraciones en las plataformas de correo que bloqueen o restrinjan reglas de reenvío automático hacia dominios no autorizados. Las configuraciones deben verificarse periódicamente y ante cambios en la plataforma. Evidencia: políticas de correo, configuraciones, registros de reglas de reenvío, alertas y reportes de revisión.
- Proteger la información física durante su transporte, mediante el uso de embalajes adecuados al tipo, clasificación y características del medio, utilizando sobres opacos, protección contra manipulación y medidas contra factores ambientales como calor, humedad o radiación electromagnética cuando corresponda. Estas medidas deben aplicarse antes de cada envío y verificarse durante la recepción. Evidencia: registros de embalaje, listas de verificación, guías de transporte, actas de entrega y recepción.
- Utilizar mecanismos inviolables o resistentes a manipulaciones para transportar información física clasificada, mediante bolsas, sobres, contenedores o mecanismos equivalentes que permitan identificar intentos de apertura o alteración durante el tránsito. El nivel de protección debe seleccionarse de acuerdo con la clasificación y criticidad de la información. Evidencia: registros de despacho, identificación del mecanismo de protección, cadena de custodia, actas de recepción y reportes de novedades.
- Mantener la trazabilidad de los envíos de información física, mediante registros que permitan identificar el contenido o tipo de información, clasificación, protección aplicada, remitente, destinatarios autorizados, fecha y hora de entrega, custodios durante el tránsito y recepción en destino. El registro debe diligenciarse para cada envío y conservarse de

acuerdo con los tiempos institucionales. Evidencia: registros de envío, guías, cadenas de custodia, firmas o constancias de recepción y reportes de novedades.

- Aplicar controles de protección de la información en las salas de reuniones, mediante el uso de espacios con acceso controlado, puertas cerradas, mecanismos de aislamiento acústico cuando se requiera, restricción de dispositivos de grabación y demás medidas definidas según la sensibilidad de la información tratada. Los controles deben aplicarse antes y durante reuniones que involucren información reservada, sensible o crítica. Evidencia: controles de acceso, reservas de salas, listas de verificación, registros de autorización y reportes de inspección.

Funcionarios y terceros

- Proteger la información institucional importante, reservada o clasificada frente a divulgación no autorizada, mediante el cumplimiento de las restricciones de acceso, etiquetado, almacenamiento, transmisión, conversación y disposición establecidas para cada nivel de clasificación. Estas medidas deben aplicarse durante todo el ciclo de vida de la información y ante cualquier forma de tratamiento físico, electrónico o verbal. Evidencia: registros de capacitación, compromisos de confidencialidad, controles de acceso, reportes de incidentes y resultados de verificaciones.
- Formalizar el compromiso de confidencialidad y no divulgación de la información reservada o clasificada, mediante la suscripción de los formatos institucionales correspondientes antes de acceder a la información, cuando así lo establezcan las políticas, contratos o requisitos legales. El compromiso debe mantenerse vigente durante la

relación y después de su terminación cuando corresponda. Evidencia: acuerdos de confidencialidad suscritos, contratos, registros de vinculación y constancias de aceptación.

- Reportar los mensajes que contengan información inapropiada, amenazante, perjudicial para la imagen institucional o fuera de contexto, mediante los canales institucionales de reporte, informando al jefe inmediato y a la autoridad competente y remitiendo el caso a Seguridad de la Información cuando pueda constituir un evento o incidente de seguridad. El reporte debe realizarse inmediatamente después de su identificación, evitando reenviar innecesariamente el contenido a destinatarios no autorizados. Evidencia: reporte o ticket, mensaje original preservado, comunicaciones, análisis y registro de tratamiento del incidente.
- Evitar el reenvío de correos electrónicos y agendas institucionales hacia cuentas personales, mediante el uso exclusivo de las plataformas institucionales autorizadas para almacenar, consultar y compartir información relacionada con las funciones. Esta condición debe cumplirse permanentemente y podrá ser verificada mediante controles técnicos y registros de correo. Evidencia: políticas de correo, registros de monitoreo, alertas de seguridad y reportes de incumplimiento.
- Realizar conversaciones que involucren información confidencial únicamente en espacios y canales autorizados, mediante la selección de lugares privados, salas con controles de seguridad o canales de comunicación institucionales que reduzcan el riesgo de escucha, interceptación o divulgación por personas no autorizadas. Esta medida debe aplicarse antes y durante cualquier conversación que involucre información clasificada. Evidencia: registros de reuniones, controles de acceso, autorizaciones de espacios y reportes de incidentes cuando se

presenten.

- Evitar incluir información confidencial o clasificada en mensajes de voz o contestadores automáticos, mediante el uso de mensajes genéricos que no revelen información institucional sensible y utilizando canales autorizados para transmitir dicha información. Esta medida debe aplicarse en cada comunicación telefónica o de voz que pueda ser consultada por terceros no autorizados. Evidencia: registros de capacitación, lineamientos de comunicación y reportes de incidentes o incumplimientos.
- Informar la clasificación y condiciones de manejo antes de iniciar conversaciones que involucren información sensible, reservada o clasificada, mediante una advertencia verbal o mecanismo equivalente que indique a los participantes el nivel de clasificación, restricciones de divulgación, prohibiciones de grabación o reproducción y demás controles aplicables. Esta advertencia debe realizarse al inicio de cada reunión o conversación en la que se trate información clasificada. Evidencia: actas o registros de reunión, listas de asistencia, controles de clasificación y, cuando corresponda, constancia de las instrucciones de manejo.

8.4.4. Derechos de propiedad intelectual (IPR)

Control Asociado en el MSPI A.5.33

Implementar procedimientos apropiados para el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de software patentado. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Fortalecer la cultura sobre los derechos de propiedad intelectual, mediante campañas de sensibilización, capacitaciones, inducción,

reinducción y comunicaciones que incluyan derechos de autor, uso legítimo de software, licenciamiento, reconocimiento de fuentes y consecuencias del uso no autorizado. Esta actividad debe realizarse como mínimo una vez al año y cuando se presenten cambios normativos, incidentes o incumplimientos relacionados con propiedad intelectual. Evidencia: Plan de capacitación, material de sensibilización, registros de asistencia, evaluaciones y comunicaciones realizadas.

- Implementar y mantener la política y los procedimientos relacionados con los derechos de propiedad intelectual, mediante la incorporación de los requisitos legales, estatutarios, reglamentarios y contractuales aplicables a derechos de autor, software, licencias, código fuente, contenidos digitales y demás activos protegidos. La documentación debe revisarse como mínimo una vez al año y cuando se presenten cambios normativos, contractuales, tecnológicos u organizacionales. Evidencia: Política y procedimientos aprobados, control de versiones, registros de revisión y evidencias de divulgación.
- Aplicar controles de navegación para restringir el acceso a sitios que puedan facilitar la infracción de derechos de autor, mediante categorías de filtrado web, listas de bloqueo y reglas configuradas en las herramientas institucionales de seguridad. Los controles deben revisarse periódicamente y actualizarse cuando se identifiquen nuevos sitios, riesgos o requerimientos legales. Evidencia: Configuraciones del filtro web, listas de bloqueo, reportes de navegación, registros de actualización y pruebas de funcionamiento.

SIDT

- Proteger la propiedad intelectual de la ANCP-CCE y de terceros, mediante controles administrativos, contractuales y tecnológicos

aplicables a derechos de autor, software, licencias, código fuente y demás contenidos protegidos. Los controles deben definirse de acuerdo con la clasificación de la información, los riesgos identificados y las condiciones de adquisición, uso o desarrollo, y deben revisarse ante cambios tecnológicos, contractuales o normativos. Evidencia: Matrices de controles, procedimientos, contratos, acuerdos de licencia, configuraciones y registros de revisión.

- Controlar el uso de software autorizado, mediante la validación del software instalado y utilizado frente al inventario institucional y las autorizaciones otorgadas, independientemente de que corresponda a software propietario, comercial, de código abierto o software libre. La verificación debe realizarse periódicamente y antes de instalar o utilizar nuevo software. Evidencia: Inventario de software, registros de autorización, reportes de herramientas de gestión y resultados de las verificaciones.
- Verificar el licenciamiento del software utilizado para actividades operativas y de desarrollo, mediante la conciliación entre el software instalado, las licencias adquiridas o autorizadas y los términos y condiciones establecidos por cada fabricante o proveedor. Esta revisión debe realizarse como mínimo una vez al año y antes de renovar, ampliar o implementar software. Evidencia: Inventario conciliado, contratos, facturas, certificados de licencia, acuerdos de uso e informes de verificación.
- Controlar el cumplimiento de los límites establecidos en las licencias de software, mediante el monitoreo periódico del número de usuarios, instalaciones, capacidad, funcionalidades y demás condiciones de utilización del software registrado en el inventario. Cuando se identifique sobreutilización, debe gestionarse su regularización, ampliación,

reducción o desinstalación, según corresponda. Evidencia: Reportes de utilización, métricas de licenciamiento, alertas, tickets de regularización y registros de acciones correctivas.

- Reportar los eventos o incidentes relacionados con posibles violaciones de derechos de propiedad intelectual, mediante los canales institucionales de gestión de incidentes, indicando como mínimo el software o contenido involucrado, activo o usuario afectado, fecha, situación identificada y evidencias disponibles. El reporte debe realizarse inmediatamente después de su identificación. Evidencia: Tickets de incidentes, reportes, evidencias técnicas y registros de seguimiento y cierre.
- Conservar las evidencias que acrediten la propiedad o derecho de uso de las licencias de software adquiridas, mediante un repositorio institucional controlado que permita asociar cada licencia con el software, fabricante o proveedor, cantidad adquirida, vigencia y condiciones de uso. La información debe actualizarse con cada adquisición, renovación, modificación o terminación. Evidencia: Contratos, facturas, certificados, registros de activación cuando aplique, acuerdos de licencia y repositorio de evidencias.
- Mantener actualizado el inventario de licenciamiento de la entidad, mediante el registro del software, fabricante, tipo de licencia, cantidad adquirida, cantidad utilizada, vigencia, responsable y condiciones de uso. El inventario debe revisarse periódicamente y actualizarse ante adquisiciones, renovaciones, bajas o cambios en el uso del software. Evidencia: Inventario de licenciamiento, registros de actualización y resultados de conciliación.
- Controlar el uso de software libre y de código abierto, mediante la identificación y revisión de las condiciones establecidas en las

respectivas licencias antes de su incorporación y durante su utilización, modificación o distribución. Cuando la licencia establezca obligaciones específicas sobre atribución, distribución, modificación o publicación del código, estas deben ser verificadas antes de realizar dichas actividades. Evidencia: Análisis de licencias, registros de aprobación, documentación técnica y evidencias de cumplimiento de sus condiciones.

- Gestionar el registro del software desarrollado por la entidad ante la autoridad competente cuando corresponda, mediante la identificación de los desarrollos susceptibles de protección, recopilación de la documentación requerida y realización del trámite de registro conforme a los requisitos aplicables. La actividad debe efectuarse una vez finalizado el desarrollo o cuando las condiciones legales o institucionales determinen su procedencia. Evidencia: Solicitud, certificado de registro, documentación del software y constancias del trámite.

Funcionarios y terceros

- Utilizar únicamente software legalmente adquirido o autorizado por la ANCP-CCE, mediante la instalación y ejecución de aplicaciones incluidas en el inventario institucional o previamente autorizadas por la Dirección de Gestión de Innovación y Tecnología. Esta condición debe cumplirse durante todo el período de utilización de los recursos tecnológicos institucionales. Evidencia: Inventario de software, registros de autorización, herramientas de gestión y reportes de verificación.
- Aplicar las políticas y lineamientos institucionales para el uso de software licenciado, mediante la utilización del software conforme a sus condiciones de licencia, restricciones de instalación, número de usuarios, funcionalidades y demás condiciones establecidas por la entidad o el fabricante. El cumplimiento debe verificarse mediante revisiones

técnicas, monitoreo y gestión de incidentes. Evidencia: Registros de aceptación de políticas, capacitaciones, inventarios, reportes de monitoreo y resultados de revisiones.

- Reconocer las fuentes de información utilizadas en presentaciones, documentos, informes y demás productos institucionales, mediante la inclusión de citas, referencias bibliográficas, autores, enlaces o mecanismos de atribución correspondientes al contenido utilizado. La verificación debe realizarse antes de la publicación, distribución o entrega del documento cuando corresponda. Evidencia: Documentos, presentaciones, informes y demás productos con las respectivas referencias o atribuciones.
- Cumplir las disposiciones legales relacionadas con los derechos de propiedad intelectual, mediante la aplicación de las normas de derechos de autor, licenciamiento, uso de contenidos, software y demás obras protegidas que sean aplicables a las actividades desarrolladas para la entidad. El cumplimiento debe mantenerse durante toda la relación laboral o contractual. Evidencia: Contratos, compromisos de propiedad intelectual, aceptación de políticas y registros de capacitación.
- Evitar la descarga, almacenamiento o ejecución de archivos sujetos a derechos de propiedad intelectual que no hayan sido autorizados para fines institucionales, mediante la aplicación de las políticas de uso aceptable, controles de navegación, restricciones de instalación y mecanismos de monitoreo establecidos por la entidad. Los controles deben mantenerse durante la utilización de los recursos tecnológicos institucionales. Evidencia: Configuraciones de seguridad, registros de navegación, alertas, reportes de monitoreo y tickets de incidentes.
- Cumplir los requisitos legales y reglamentarios relacionados con propiedad intelectual, protección de registros, privacidad, datos

personales y controles criptográficos, mediante la aplicación de las políticas institucionales, procedimientos, acuerdos contractuales y controles establecidos para cada actividad. El cumplimiento debe verificarse durante la ejecución de los procesos y cuando se presenten cambios normativos o contractuales. Evidencia: Políticas aceptadas, contratos, registros de capacitación, evaluaciones de cumplimiento y evidencias de aplicación de controles.

- Prevenir la copia, reproducción o distribución no autorizada de software o documentación protegida, mediante la aplicación de las restricciones establecidas en las licencias, controles de acceso, permisos sobre repositorios, restricciones de copia y mecanismos de monitoreo, cuando sean técnicamente aplicables. Antes de copiar, modificar o distribuir software o documentación debe verificarse la autorización correspondiente. Evidencia: Licencias, autorizaciones, registros de acceso, configuraciones de seguridad, logs y evidencias de revisión.

8.4.5. Protección de registros

Control Asociado en el MSPI A.5.34

Asegurar que los registros sean protegidos contra pérdidas, alteraciones o accesos no autorizados. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Gestionar la protección de los registros almacenados en bases de datos, registros de transacciones (Logs) y registros de auditoría (Audit Logs), mediante la definición, documentación y aplicación de lineamientos, procedimientos e instructivos que establezcan como mínimo los controles de acceso, integridad, disponibilidad, trazabilidad, almacenamiento, conservación, consulta, respaldo y disposición. Estos documentos deben revisarse como mínimo una vez al año y cuando se

presenten cambios tecnológicos, normativos, contractuales, de infraestructura o de los riesgos asociados. Evidencia: Lineamientos, procedimientos, instructivos, registros de revisión y aprobación.

- Implementar sistemas de almacenamiento y gestión de datos, mediante plataformas y mecanismos que permitan controlar el acceso, conservación, recuperación, integridad, disponibilidad y disposición de los registros durante todo su ciclo de vida. La capacidad y configuración de estos sistemas debe revisarse periódicamente y cuando se incorporen nuevas fuentes de información o cambien los requisitos de conservación. Evidencia: Arquitecturas, configuraciones, inventario de sistemas de almacenamiento, procedimientos y registros de revisión.
- Mantener la legibilidad y accesibilidad de los registros durante todo el período de retención, mediante el uso de formatos, medios y tecnologías compatibles con los períodos de conservación definidos y mediante procesos de migración, conversión o actualización tecnológica cuando exista riesgo de obsolescencia. La accesibilidad debe verificarse periódicamente y antes de realizar cambios tecnológicos que puedan afectar la consulta de la información. Evidencia: Pruebas de acceso y lectura, registros de migración o conversión, controles de integridad y reportes de verificación.
- Permitir la recuperación de los datos dentro de los tiempos y formatos requeridos, mediante mecanismos de respaldo, restauración, recuperación y conversión que consideren los requisitos legales, contractuales, operativos y de continuidad aplicables a cada registro. Las capacidades de recuperación deben probarse periódicamente y cuando se modifiquen las plataformas o requisitos de recuperación. Evidencia: Procedimientos de recuperación, registros de pruebas de restauración, resultados de pruebas, tiempos de recuperación y reportes de

cumplimiento.

- Identificar los registros y determinar su período de retención, mediante la asociación de cada tipo de registro con su proceso, activo de información, clasificación, serie o subserie documental cuando aplique y período de conservación definido en el Programa de Gestión Documental y demás requisitos legales, reglamentarios o contractuales. La información debe revisarse cuando se creen nuevos registros o se modifiquen los requisitos de conservación. Evidencia: Inventario de registros, tablas de retención documental, matrices de conservación y registros de actualización.
- Ejecutar la disposición o destrucción de registros que hayan cumplido su período de retención, mediante procedimientos autorizados que verifiquen previamente que no existan obligaciones legales, contractuales, administrativas, investigaciones o necesidades institucionales que exijan su conservación. La destrucción debe realizarse utilizando mecanismos acordes con el medio y clasificación de la información y dejando constancia de la actividad. Evidencia: Autorizaciones de disposición, actas de eliminación, registros de destrucción y soportes de verificación.
- Documentar y mantener actualizados los procedimientos para la retención, almacenamiento, manejo y disposición de registros electrónicos, mediante la integración de los requisitos tecnológicos y de seguridad con las disposiciones establecidas en el Programa de Gestión Documental de la ANCP-CCE. Los documentos deben revisarse como mínimo anualmente y ante cambios normativos, tecnológicos o documentales. Evidencia: Procedimientos aprobados, control de versiones, registros de revisión y divulgación.
- Implementar el programa de retención de registros electrónicos,

mediante la identificación de los tipos de registros, responsables, período de conservación, medio de almacenamiento, condiciones de acceso y disposición final. El programa debe mantenerse actualizado cuando se incorporen nuevos sistemas, registros, procesos o requisitos legales. Evidencia: Programa de retención, matriz de registros, inventarios y registros de actualización.

- Mantener un inventario de las fuentes de información, mediante la identificación y registro de bases de datos, aplicaciones, sistemas, dispositivos, servicios tecnológicos, repositorios y demás fuentes que generen, procesen o almacenen información, asociándolas con los activos de información y su clasificación institucional. El inventario debe actualizarse ante la incorporación, modificación, migración o retiro de fuentes de información. Evidencia: Inventario de fuentes, inventario de activos de información, matrices de clasificación y registros de actualización.
- Aplicar los requisitos estatutarios, reglamentarios, contractuales y misionales para la conservación y gestión de registros electrónicos, mediante procedimientos que definan los períodos de retención, condiciones de almacenamiento, controles de acceso, mecanismos de protección, recuperación y disposición, tomando como referencia el Programa de Gestión Documental de la ANCP-CCE. El cumplimiento debe verificarse periódicamente y ante cambios en los requisitos aplicables. Evidencia: Procedimientos, matrices de requisitos, registros de cumplimiento, informes de revisión y evidencias de aplicación de controles.
- Proteger los registros de eventos generados por el hardware y software de la infraestructura de seguridad, mediante su almacenamiento en repositorios seguros, con acceso restringido mediante autenticación y

autorización, protección contra modificación o eliminación no autorizada, mecanismos de respaldo y controles de trazabilidad. Los permisos de acceso deben revisarse periódicamente y ante cambios de personal, roles, sistemas o incidentes de seguridad. Evidencia: Configuraciones de repositorios y herramientas de gestión de logs, matrices de acceso, registros de auditoría, respaldos y reportes de revisión.

- Reportar los eventos o incidentes relacionados con pérdida, destrucción, falsificación, acceso no autorizado o liberación no autorizada de registros, mediante los canales institucionales de gestión de incidentes, suministrando como mínimo el registro o sistema afectado, fecha y hora, situación identificada, posible impacto, usuarios involucrados y evidencias disponibles. El reporte debe realizarse inmediatamente después de su identificación y debe mantenerse seguimiento hasta su cierre. Evidencia: Tickets de incidentes, registros de eventos, evidencias técnicas, informes de análisis y registros de seguimiento y cierre.

Funcionarios y terceros

- Aplicar los lineamientos establecidos en el Programa de Gestión Documental de la ANCP-CCE para el manejo de registros e información, mediante el cumplimiento de las disposiciones relacionadas con creación, clasificación, organización, almacenamiento, consulta, acceso, conservación, transferencia y disposición de los registros bajo su responsabilidad. El cumplimiento debe observarse durante todo el ciclo de vida del registro y verificarse mediante revisiones, auditorías o controles establecidos por la entidad. Evidencia: Registros documentales, controles de acceso, transferencias documentales, actas de disposición, registros de capacitación y resultados de verificaciones.

8.4.6. Privacidad y protección de información personal identificable (PII)

Control Asociado en el MSPI A.5.36

Mantener la protección y privacidad de la información de datos personales tal como lo estipula la legislación, las regulaciones y, si fuese aplicable, las cláusulas contractuales. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Actualizar y verificar el cumplimiento de la Política de Protección de Datos Personales y de la documentación asociada, mediante revisiones periódicas de su contenido frente a cambios normativos, organizacionales, tecnológicos, contractuales y de tratamiento de datos personales. La documentación debe revisarse como mínimo una vez al año y cada vez que se presenten cambios que puedan afectar las condiciones de tratamiento o protección de los datos. Evidencia: Política actualizada, control de versiones, matriz de requisitos, registros de revisión, aprobaciones y resultados de verificaciones de cumplimiento.
- Implementar lineamientos y controles para prevenir la divulgación, circulación o acceso no autorizado a datos personales, mediante compromisos de confidencialidad, controles de acceso basados en roles y necesidad de conocer, definición de responsabilidades, anonimización o seudonimización cuando aplique, cifrado, controles de transferencia y mecanismos de monitoreo. Los controles deben definirse antes de iniciar el tratamiento y revisarse periódicamente o cuando cambien los riesgos, sistemas, procesos o medios de tratamiento. Evidencia: Lineamientos, acuerdos de confidencialidad, matrices de acceso, configuraciones de seguridad, procedimientos de anonimización/cifrado y registros de revisión.

Jefes de dependencias

- Identificar y gestionar los riesgos de seguridad de la información asociados a los activos que contengan datos personales, mediante la identificación de amenazas, vulnerabilidades, impactos sobre confidencialidad, integridad y disponibilidad, valoración del riesgo y definición de controles y acciones de tratamiento. La evaluación debe realizarse como mínimo anualmente y cuando se incorporen nuevos activos, tratamientos, sistemas, terceros, tecnologías o se presenten incidentes o cambios significativos. Evidencia: Inventario de activos, matriz de riesgos, planes de tratamiento, registros de seguimiento y evidencias de implementación de controles.
- Aplicar obligatoriamente los requisitos de protección de datos personales en el diseño, implementación o modificación de servicios y procesos, mediante una revisión previa de privacidad y seguridad que considere nuevos canales de atención, procesos, espacios físicos, interoperabilidad, sistemas, servicios digitales y mecanismos de circulación interna o externa de información. La revisión debe realizarse antes de la puesta en operación y nuevamente cuando se presenten cambios significativos. Evidencia: Listas de verificación, análisis de privacidad, requisitos de seguridad, conceptos de revisión, actas y aprobaciones previas a la puesta en producción.
- Identificar los activos de información que contienen datos personales, mediante la revisión del inventario de activos y el registro de la naturaleza de los datos tratados, responsable del activo, proceso asociado, finalidad y condiciones de tratamiento. La identificación debe realizarse durante la creación o actualización del inventario y revisarse como mínimo anualmente o cuando cambien los tratamientos.

Evidencia: Inventario de activos de información, matriz de datos personales y registros de actualización.

- Identificar los medios físicos y electrónicos en los que se encuentran los datos personales, mediante el registro de bases de datos, aplicaciones, sistemas, documentos físicos, dispositivos, repositorios y demás medios utilizados para su almacenamiento o tratamiento. La información debe actualizarse cuando se incorporen, modifiquen, migren o eliminen medios de tratamiento. Evidencia: Inventario de medios, diagramas de flujo de información, registros de sistemas y matrices de tratamiento.
- Determinar y aplicar las medidas de seguridad correspondientes a los activos que contienen datos personales, mediante la evaluación de su clasificación, criticidad, riesgos, tipo de información y operaciones de tratamiento, definiendo controles de acceso, autenticación, cifrado, respaldo, monitoreo, trazabilidad y demás medidas aplicables. Los controles deben revisarse periódicamente y ante cambios en los riesgos o tratamientos. Evidencia: Matrices de riesgos y controles, configuraciones, registros de acceso, reportes de monitoreo y resultados de verificaciones.
- Verificar que la recolección, tratamiento, almacenamiento, circulación y disposición de los datos personales se realicen conforme a la normatividad y políticas institucionales, mediante listas de verificación, revisiones de procesos, validación de autorizaciones y análisis de los mecanismos utilizados para cada operación de tratamiento. La verificación debe realizarse periódicamente y cuando se implementen nuevos tratamientos o se modifiquen los existentes. Evidencia: Listas de verificación, informes de revisión, autorizaciones, registros de tratamiento y planes de mejora.
- Evaluar la obligación de registrar las bases de datos con información

personal en el Registro Nacional de Bases de Datos (RNBD), mediante la revisión de los criterios y condiciones establecidos por la Superintendencia de Industria y Comercio y la validación de las características de cada base de datos. Cuando resulte aplicable, debe gestionarse el registro y mantenerse actualizada la información y los reportes requeridos dentro de los plazos establecidos. Evidencia: Análisis de aplicabilidad, registros en el RNBD, constancias de actualización y reportes presentados.

- Controlar directamente el tratamiento de los datos personales bajo responsabilidad de la dependencia o delegarlo formalmente a un tercero, mediante la definición previa de responsabilidades, finalidades, instrucciones de tratamiento, controles de seguridad, deberes de confidencialidad, condiciones de acceso, transferencia, devolución y eliminación. Antes de permitir el acceso de un tercero debe verificarse el cumplimiento de los requisitos contractuales y de seguridad aplicables. Evidencia: Contratos, acuerdos de tratamiento de datos, cláusulas de confidencialidad, matrices de responsabilidades, autorizaciones y evaluaciones de terceros.
- Aplicar los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad durante el tratamiento de datos personales, mediante la validación de la finalidad y base jurídica del tratamiento, obtención de las autorizaciones requeridas, control de acceso, actualización de información, restricción de circulación y aplicación de medidas de seguridad durante todo el ciclo de vida de los datos. Evidencia: Autorizaciones, avisos de privacidad, registros de tratamiento, matrices de acceso, controles de seguridad y resultados de verificaciones.

Todas las dependencias, funcionarios y terceros

- Cumplir la normatividad nacional y los lineamientos institucionales sobre protección de datos personales, mediante la aplicación de las políticas, procedimientos, controles y obligaciones definidos por la ANCP-CCE durante la recolección, tratamiento, almacenamiento, consulta, transferencia y disposición de los datos. El cumplimiento debe mantenerse durante todo el ciclo de vida de la información y verificarse mediante controles, auditorías o revisiones institucionales. Evidencia: Registros de tratamiento, autorizaciones, capacitaciones, controles de acceso, informes de auditoría y evidencias de cumplimiento.
- Suprimir o disponer los datos personales cuando se hayan cumplido las finalidades del tratamiento, mediante la aplicación de los procedimientos de eliminación, destrucción o disposición documental definidos por la entidad, previa verificación de que no existan obligaciones legales, contractuales, administrativas, judiciales o de conservación que exijan mantenerlos. La disposición debe ejecutarse conforme al Programa de Gestión Documental y dejar evidencia de la actividad. Evidencia: Actas de eliminación, registros de disposición documental, autorizaciones y evidencias técnicas de eliminación segura.
- Mantener actualizada la información personal, mediante la aplicación de controles de validación, actualización y corrección de los datos y la atención de las solicitudes de los titulares conforme a los procedimientos institucionales. La revisión debe realizarse durante el tratamiento y cuando se identifiquen inconsistencias, solicitudes de actualización o cambios en la información. Evidencia: Registros de actualización, solicitudes de titulares, trazabilidad de modificaciones y controles de calidad de datos.
- Recolectar únicamente los datos personales necesarios para cumplir las

funciones y finalidades autorizadas, mediante la definición previa de los datos requeridos, la justificación de su necesidad y la eliminación de campos o información que no sean indispensables para el tratamiento. Esta validación debe realizarse antes de crear o modificar formularios, sistemas, servicios o mecanismos de recolección de información. Responsable: Evidencia: Formularios, matrices de datos recolectados, análisis de necesidad, avisos de privacidad y registros de revisión.

- Aplicar medidas técnicas y administrativas para proteger los datos personales durante su tratamiento, mediante controles de autenticación, autorización, gestión de privilegios, cifrado cuando corresponda, respaldo, monitoreo, trazabilidad, protección física, capacitación y gestión de incidentes. Los controles deben mantenerse durante todo el ciclo de vida de los datos y revisarse periódicamente o ante cambios en los riesgos. Evidencia: Configuraciones de seguridad, matrices de acceso, logs, reportes de monitoreo, registros de capacitación, evaluaciones y pruebas de controles.

8.4.7. Trabajo a distancia

Control Asociado en el MSPI A.6.7

Garantizar seguridad de la información cuando el personal trabaja a distancia. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Socializar las medidas de seguridad, privacidad y buenas prácticas aplicables al teletrabajo, mediante jornadas de capacitación, inducción, reinducción, campañas y comunicaciones que incluyan protección de información, gestión de contraseñas, uso seguro de equipos y redes, prevención de fuga de información, manejo de información pública clasificada y reservada, reporte de incidentes y protección de datos personales. La socialización debe realizarse antes del inicio del

teletrabajo y reforzarse como mínimo anualmente o cuando se presenten cambios en los controles o riesgos identificados. Evidencia: Material de capacitación, registros de asistencia, evaluaciones, comunicaciones y constancias de socialización.

- Comunicar las medidas de seguridad de la información que deben cumplir los teletrabajadores, mediante la entrega y publicación de lineamientos específicos para el acceso remoto, uso de dispositivos, conexiones, almacenamiento, transferencia de información, protección de credenciales y reporte de incidentes. La comunicación debe realizarse antes de habilitar el acceso remoto y actualizarse cuando cambien los requisitos de seguridad. Evidencia: Lineamientos publicados, comunicaciones, constancias de aceptación y registros de divulgación.

La SIDT

- Mantener identificado y controlado el inventario de equipos asignados a teletrabajadores, mediante el registro del usuario responsable, identificación del equipo, serial, características, sistema operativo, ubicación de uso, estado, fecha de asignación y devolución. El inventario debe actualizarse con cada asignación, cambio, mantenimiento, pérdida, retiro o devolución del equipo. Evidencia: Inventario de activos, actas de entrega y devolución, registros de asignación y tickets de soporte.
- Implementar controles tecnológicos para proteger la confidencialidad, integridad y disponibilidad de la información durante el teletrabajo, mediante autenticación robusta, control de acceso, protección de endpoint, cifrado, VPN o mecanismos equivalentes, antivirus/EDR, firewall, actualización de sistemas, protección contra malware y monitoreo de eventos. Los controles deben aplicarse antes de habilitar el equipo y mantenerse durante todo el período de teletrabajo.

Evidencia: Configuraciones de seguridad, políticas aplicadas, registros de autenticación, reportes de EDR/antimalware, VPN y monitoreo.

- Verificar la correcta configuración de los controles tecnológicos y parámetros de seguridad de los equipos utilizados para teletrabajo, mediante listas de verificación técnicas, herramientas de gestión y revisión de configuraciones de seguridad. La verificación debe realizarse antes de habilitar el acceso remoto, periódicamente y después de cambios relevantes o incidentes de seguridad. Evidencia: Listas de verificación, reportes de configuración, resultados de escaneos, tickets y registros de remediación.
- Proteger la transmisión de información durante el teletrabajo, mediante el uso de protocolos seguros, canales institucionales, VPN, cifrado en tránsito, autenticación y controles de acceso que impidan la interceptación o modificación no autorizada de la información. Estos mecanismos deben utilizarse en toda conexión o transferencia de información hacia los recursos institucionales. Evidencia: Configuración de VPN y protocolos seguros, certificados, registros de conexión, configuraciones de cifrado y pruebas técnicas.
- Verificar periódicamente la efectividad de los controles aplicados a las conexiones remotas, mediante el análisis de registros de autenticación, conexiones VPN, eventos de seguridad, intentos fallidos, accesos anómalos y alertas generadas por las herramientas de seguridad. La revisión debe realizarse periódicamente y ante incidentes, cambios de infraestructura o alertas de seguridad. Evidencia: Logs, reportes de monitoreo, informes de revisión, alertas y tickets de incidentes.
- Mantener una línea base de software y configuración de seguridad en los equipos utilizados para teletrabajo, mediante imágenes, perfiles de configuración, políticas de gestión de dispositivos y herramientas de

administración centralizada que permitan aplicar las mismas condiciones de seguridad definidas para los equipos institucionales. La línea base debe actualizarse cuando se modifiquen los estándares tecnológicos o de seguridad. Evidencia: Línea base documentada, imágenes de referencia, políticas de configuración, reportes de cumplimiento y registros de actualización.

- Proporcionar a los teletrabajadores los recursos tecnológicos requeridos para desarrollar sus funciones, mediante la asignación controlada de equipos, software, aplicaciones, conexiones, herramientas de colaboración y demás recursos previamente autorizados y configurados con los controles de seguridad institucionales. La asignación debe realizarse antes del inicio de las actividades y mantenerse durante la vigencia de la modalidad de teletrabajo. Evidencia: Actas de entrega, inventarios, solicitudes de servicio, registros de asignación y licenciamiento.
- Verificar que la conexión utilizada por el teletrabajador sea técnicamente apta para acceder a los servicios institucionales, mediante la validación de capacidad, estabilidad, seguridad de la conexión y condiciones mínimas requeridas para los servicios utilizados. La verificación debe realizarse antes de habilitar el acceso remoto y cuando se presenten problemas de conectividad o cambios relevantes. Evidencia: Registros de pruebas de conectividad, tickets de soporte, resultados de validaciones y autorizaciones de acceso.
- Proporcionar plataformas y herramientas institucionales para facilitar la comunicación y colaboración con los teletrabajadores, mediante soluciones autorizadas que incorporen autenticación, control de acceso, protección de información y mecanismos de trazabilidad. Las herramientas deben evaluarse antes de su implementación y cuando se

presenten cambios significativos en sus funcionalidades o riesgos. Evidencia: Inventario de herramientas autorizadas, configuraciones, contratos, evaluaciones de seguridad y registros de uso.

- Activar y conservar los registros de auditoría de los sistemas y aplicaciones utilizados por los teletrabajadores, mediante la generación, almacenamiento y protección de logs relacionados con autenticaciones, accesos, modificaciones, conexiones remotas y actividades relevantes. Los registros deben mantenerse durante el período definido institucionalmente y revisarse de acuerdo con los riesgos y necesidades de monitoreo. Evidencia: Logs, configuraciones de auditoría, reportes de monitoreo, alertas y registros de análisis.
- Implementar cifrado en los equipos utilizados para teletrabajo, mediante mecanismos de cifrado de disco, archivos o dispositivos de almacenamiento, de acuerdo con la clasificación y criticidad de la información tratada. El cifrado debe verificarse antes de entregar el equipo y mantenerse activo durante todo el período de asignación. Evidencia: Configuración de cifrado, reportes de cumplimiento, políticas de seguridad y registros de verificación.
- Implementar mecanismos de borrado remoto en los equipos que lo permitan, mediante herramientas de administración de dispositivos que permitan bloquear, localizar o eliminar la información institucional ante pérdida, robo o compromiso del equipo. El mecanismo debe mantenerse habilitado durante la asignación del equipo y ejecutarse cuando se confirme una situación que pueda comprometer la información. SIDT. Evidencia: Configuración de administración remota, políticas aplicadas, registros de activación y reportes de borrado o bloqueo.
- Asignar espacios institucionales para el almacenamiento y respaldo de información de los teletrabajadores, mediante repositorios corporativos

con controles de autenticación, autorización, clasificación, respaldo y trazabilidad, evitando que la información institucional se almacene exclusivamente en dispositivos locales. La configuración debe realizarse al inicio del teletrabajo y revisarse periódicamente. Evidencia: Permisos de acceso, registros de almacenamiento, configuraciones de respaldo, logs y reportes de utilización.

Funcionarios en modalidad de teletrabajo

- Proteger las cuentas de usuario y contraseñas utilizadas para acceder a equipos, aplicaciones y redes institucionales, mediante el uso exclusivo de credenciales personales, contraseñas robustas, autenticación multifactor cuando esté disponible y mecanismos de bloqueo ante intentos no autorizados. Las credenciales no deben compartirse y cualquier sospecha de compromiso debe reportarse inmediatamente. Evidencia: Registros de autenticación, configuraciones de MFA, políticas aceptadas y reportes de incidentes.
- Mantener la trazabilidad y responsabilidad sobre las actividades realizadas con su cuenta de usuario, mediante el uso exclusivo de las credenciales asignadas y evitando su préstamo, divulgación o utilización por terceros. Ante la identificación de una actividad no realizada por el titular, debe reportarse inmediatamente a la SIDT o mediante el canal institucional de incidentes. Evidencia: Logs de autenticación y actividad, reportes de incidentes y registros de seguimiento.
- Proteger la información generada, recibida, adquirida o administrada durante el desarrollo de las funciones, mediante la aplicación de los controles establecidos según su clasificación, incluyendo restricciones de acceso, almacenamiento seguro, cifrado, transferencia mediante canales

autorizados y prevención de copias no autorizadas, especialmente cuando se trate de información pública clasificada o reservada. Estas medidas deben aplicarse durante todo el ciclo de vida de la información. Evidencia: Registros de acceso, repositorios institucionales, controles de transferencia, cifrado y reportes de monitoreo.

- Preservar la configuración de seguridad de los equipos asignados, mediante la prohibición de instalar software, aplicaciones o programas que no hayan sido autorizados por la entidad y mediante el uso de los mecanismos institucionales de administración y protección de equipos. Esta condición debe mantenerse durante toda la asignación del equipo. Evidencia: Inventario de software, reportes de gestión de dispositivos, alertas de instalación y registros de soporte.
- Utilizar los equipos suministrados por la ANCP-CCE exclusivamente para las funciones institucionales autorizadas, mediante la aplicación de las políticas de uso aceptable y las restricciones técnicas configuradas por la SIDT. El cumplimiento podrá ser verificado mediante mecanismos de monitoreo y auditoría institucional. Evidencia: Políticas aceptadas, registros de monitoreo, logs y reportes de auditoría.
- Presentar los equipos asignados para teletrabajo cuando la SIDT lo requiera, mediante la entrega física o disponibilidad para revisión técnica, mantenimiento, actualización, diagnóstico, inventario o aplicación de controles de seguridad, dentro de los plazos establecidos en la solicitud. Responsable: Teletrabajador. Evidencia: Solicitudes de servicio, actas de entrega/recepción, tickets de soporte y registros de mantenimiento.
- Evitar el uso compartido de los equipos y recursos tecnológicos institucionales, mediante el uso individual de las cuentas de usuario y la configuración de mecanismos de autenticación que impidan el acceso de

personas no autorizadas. Esta condición debe mantenerse durante todo el período de asignación. Evidencia: Registros de autenticación, configuraciones de cuentas, políticas aceptadas y resultados de verificaciones.

- Formalizar el compromiso de cumplimiento de las condiciones de seguridad para el teletrabajo, mediante la suscripción y aceptación del acuerdo correspondiente antes de iniciar esta modalidad de trabajo y cada vez que se modifiquen sustancialmente sus condiciones de seguridad. Evidencia: Acuerdo de seguridad firmado o aceptado, registros de aceptación y control documental.

8.4.8. Dispositivos terminales de usuario

Control Asociado en el MSPI A.8.1

Definir los parámetros y medidas de seguridad que deben implementar los funcionarios y terceros de la ANCP-CCE para proteger los dispositivos de punto final de usuario y la información procesada y almacenada en estos, de tal manera que estén resguardados de pérdida, daño, acceso o divulgación no autorizada. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Autorizar, entregar y controlar el uso de dispositivos móviles y de punto final, mediante la validación previa del perfil del cargo, funciones, necesidades de la dependencia y autorización técnica emitida por la SIDT. La asignación debe realizarse antes de la entrega del dispositivo y revisarse cuando cambie el cargo, dependencia, función o necesidad que originó la asignación. Evidencia: Solicitud y autorización de asignación, acta de entrega, inventario de activos y registros de devolución o reasignación.

- Implementar controles de cifrado para los dispositivos de punto final, mediante mecanismos de cifrado de disco, almacenamiento o archivos, de acuerdo con la clasificación y sensibilidad de la información procesada o almacenada. El cifrado debe verificarse antes de la entrega del dispositivo y mantenerse durante todo su ciclo de vida o mientras procese información institucional que requiera protección. Evidencia: Políticas de cifrado, configuraciones, reportes de cumplimiento y registros de verificación.
- Controlar el ingreso y salida de dispositivos de punto final de las instalaciones, mediante procedimientos que permitan identificar el dispositivo, usuario responsable, fecha, hora, motivo de salida o ingreso y autorización correspondiente. Los controles deben aplicarse cada vez que un dispositivo sea retirado o ingresado a las instalaciones. Evidencia: Registros de salida y entrada, autorizaciones, inventarios y controles de seguridad física.
- Proteger la custodia, conservación, operación y mantenimiento de los dispositivos de punto final, mediante lineamientos sobre transporte, almacenamiento, manipulación, mantenimiento, actualización, protección física y uso de dispositivos personales que procesen información institucional. Los lineamientos deben aplicarse durante todo el ciclo de vida del dispositivo y revisarse ante cambios tecnológicos o de seguridad. Evidencia: Lineamientos, procedimientos, registros de mantenimiento, inventarios, actas de entrega y verificaciones de cumplimiento.
- Controlar el acceso a aplicaciones y sistemas institucionales desde dispositivos de punto final, mediante autenticación, autorización basada en roles, mínimo privilegio, autenticación multifactor cuando aplique,

gestión de sesiones y restricciones de acceso según el nivel de riesgo. Los permisos deben revisarse periódicamente y cuando cambien los roles, usuarios, aplicaciones o condiciones de acceso. Evidencia: Matrices de acceso, configuraciones de autenticación, registros de autorización, logs y reportes de revisión.

- Verificar los requisitos de seguridad de los medios removibles utilizados para acceder a información desde redes externas, mediante la validación de autorización, cifrado cuando aplique, protección contra malware, integridad del medio y restricciones de lectura o escritura. La verificación debe realizarse antes de autorizar su uso y ante cambios en los riesgos o condiciones de conexión. Evidencia: Registros de autorización, políticas de dispositivos removibles, configuraciones de seguridad, reportes de análisis y registros de uso.
- Proteger los dispositivos móviles utilizados para actividades institucionales, mediante la instalación y actualización de software autorizado, antimalware cuando técnicamente aplique, controles de configuración, bloqueo automático, cifrado y autenticación multifactor para los servicios que lo permitan. Los controles deben verificarse antes de autorizar el dispositivo y periódicamente durante su utilización. Evidencia: Inventario de dispositivos, configuraciones, reportes de cumplimiento, registros de actualización y evidencias de MFA.
- Controlar las conexiones de visitantes y usuarios internos que ingresen a las instalaciones con dispositivos personales, mediante redes segregadas, autenticación, restricciones de acceso, políticas de uso y mecanismos de monitoreo que impidan el acceso no autorizado a las redes o recursos institucionales. Los controles deben aplicarse cada vez que un dispositivo personal se conecte a la infraestructura institucional. Evidencia: Configuraciones de redes, políticas de acceso, registros de

autenticación, logs y reportes de monitoreo.

- Monitorear los dispositivos móviles institucionales y personales que procesen o accedan a activos de información, mediante las herramientas institucionales de gestión tecnológica, administración de dispositivos, protección de endpoint y registro de eventos, de acuerdo con las autorizaciones y condiciones establecidas. El monitoreo debe mantenerse durante el período en que el dispositivo tenga acceso a recursos institucionales. Evidencia: Registros de gestión de dispositivos, inventarios, logs, alertas y reportes de monitoreo.
- Realizar verificaciones remotas de los dispositivos de punto final cuando exista una necesidad técnica, de seguridad o soporte, mediante herramientas de administración remota autorizadas que permitan consultar configuraciones, estado de seguridad, software instalado y eventos relevantes. La verificación debe ejecutarse conforme a los procedimientos institucionales y generar un reporte de las actividades realizadas, respetando las condiciones legales y de privacidad aplicables. Evidencia: Tickets de soporte, registros de conexión remota, reportes técnicos, logs y resultados de la verificación.
- Proporcionar elementos de seguridad física para los dispositivos de punto final, como guayas de seguridad u otros mecanismos equivalentes, mediante la evaluación de la ubicación, criticidad del equipo y riesgo de pérdida o hurto. La asignación debe realizarse cuando el análisis determine la necesidad y verificarse durante las revisiones físicas de los activos. Evidencia: Actas de entrega, inventario de elementos de seguridad, registros de inspección y fotografías o informes de verificación cuando corresponda.
- Brindar soporte técnico a los usuarios responsables de dispositivos de punto final, mediante los canales institucionales de mesa de ayuda y

dentro de las instalaciones de la entidad, para los aplicativos y sistemas instalados en los equipos suministrados. El soporte debe ejecutarse previa generación del requerimiento y conforme a los niveles de servicio establecidos. Evidencia: Tickets de mesa de ayuda, registros de atención, diagnóstico, solución aplicada y cierre del requerimiento.

- Registrar todos los requerimientos relacionados con dispositivos de punto final, mediante la herramienta institucional de gestión de mesa de ayuda, incluyendo usuario, equipo, solicitud, diagnóstico, acciones realizadas, responsable y fecha de cierre. El registro debe efectuarse para cada atención de soporte. Evidencia: Tickets y reportes de la herramienta de mesa de ayuda.
- Reportar a Seguridad de la Información los eventos o incidentes relacionados con pérdida, daño, robo o compromiso de dispositivos de punto final, mediante los canales institucionales de gestión de incidentes, indicando como mínimo el dispositivo afectado, usuario responsable, fecha, ubicación o circunstancia conocida, información potencialmente comprometida y acciones realizadas. El reporte debe efectuarse inmediatamente después de identificar el evento. Evidencia: Ticket de incidente, reporte de seguridad, logs, evidencias técnicas y registros de seguimiento.
- Configurar el bloqueo automático de pantalla en los computadores institucionales, mediante políticas centralizadas del sistema operativo o herramientas de administración de dispositivos, estableciendo un tiempo máximo de cinco minutos de inactividad. La configuración debe aplicarse a todos los equipos institucionales y verificarse periódicamente mediante herramientas de gestión. Evidencia: Política de configuración, reportes de cumplimiento, registros de administración y resultados de pruebas.
- Aplicar procedimientos para conservar la información antes de

formatear, reinstalar o reasignar un dispositivo, mediante la identificación de la información institucional, ejecución de las copias de respaldo requeridas, validación de su disponibilidad y posterior formateo o reinstalación de las aplicaciones y servicios autorizados. El procedimiento debe ejecutarse antes de entregar el equipo a un nuevo responsable o realizar una reinstalación que implique eliminación de información. Evidencia: Registros de respaldo, actas de entrega, tickets, reportes de formateo/reinstalación y validación de restauración cuando aplique.

Funcionarios y terceros

- Solicitar autorización para utilizar aplicaciones institucionales desde dispositivos personales, mediante el registro de la solicitud ante la SIDT, indicando dispositivo, aplicación, finalidad, información a la que se accederá y condiciones de uso. La autorización debe obtenerse antes de instalar o utilizar la aplicación y mantenerse vigente mientras exista acceso institucional. Evidencia: Solicitud, autorización, inventario de dispositivos autorizados y registros de configuración.
- Permitir la habilitación de funcionalidades de auditoría y control sobre la información almacenada en dispositivos asignados, mediante la aceptación de las políticas institucionales y de los mecanismos técnicos de monitoreo, registro, administración y protección implementados por la entidad. Estas funcionalidades deben permanecer habilitadas mientras el dispositivo se encuentre bajo asignación institucional o tenga acceso a recursos de la entidad. Evidencia: Aceptación de políticas, configuraciones de gestión, logs y reportes de cumplimiento.
- Aplicar medidas de custodia, conservación, operación y mantenimiento de los dispositivos de punto final, mediante la protección física, uso

adecuado, actualización, cuidado durante el transporte, prevención de acceso de terceros y cumplimiento de los controles técnicos y administrativos establecidos por Seguridad de la Información y la SIDT. Las medidas deben aplicarse durante todo el período de asignación o utilización del dispositivo. Evidencia: Actas de entrega, inventarios, registros de mantenimiento, reportes de soporte y verificaciones de cumplimiento.

- Proteger los dispositivos de punto final durante su transporte fuera de las instalaciones, mediante su custodia directa, almacenamiento seguro, protección contra golpes, pérdida, hurto o acceso no autorizado y aplicación de los controles de cifrado y bloqueo establecidos por la entidad. Estas medidas deben aplicarse cada vez que el dispositivo sea trasladado fuera de las instalaciones. Evidencia: Acta de asignación, registros de salida, reportes de incidentes y verificaciones de activos.
- Cumplir los lineamientos de ingreso y salida de dispositivos de punto final, mediante el registro y autorización establecidos por la SIDT y los controles de seguridad física de la entidad. El procedimiento debe aplicarse en cada ingreso o salida del dispositivo. Evidencia: Registros de ingreso y salida, autorizaciones y controles de seguridad física.
- Custodiar las llaves y mecanismos de seguridad asignados para proteger los dispositivos, mediante su conservación bajo responsabilidad del usuario y evitando su préstamo o entrega a personas no autorizadas. La pérdida o deterioro debe reportarse inmediatamente para gestionar su reposición o cambio. Evidencia: Actas de entrega, registros de asignación, inventario de llaves y reportes de pérdida o reposición.
- Aplicar mecanismos de cifrado para proteger información pública clasificada y pública reservada, mediante las herramientas institucionales de cifrado autorizadas y de acuerdo con la clasificación de

la información y los lineamientos técnicos establecidos. El cifrado debe utilizarse antes de almacenar, transportar o transferir información que requiera dicha protección. Evidencia: Configuraciones de cifrado, reportes de cumplimiento y registros de verificación.

- Reportar inmediatamente la pérdida, daño, robo o compromiso de los dispositivos de punto final asignados, mediante los canales institucionales definidos para la gestión de incidentes, suministrando la información disponible sobre el equipo, circunstancias, ubicación, información potencialmente comprometida y acciones realizadas. Evidencia: Ticket de incidente, reporte al área responsable, evidencias y registros de seguimiento.
- Bloquear la pantalla del computador cuando el usuario se ausente de su puesto de trabajo, mediante la combinación de bloqueo manual o el mecanismo automático configurado institucionalmente, evitando que terceros puedan acceder a la información disponible. La medida debe aplicarse cada vez que el usuario se retire temporalmente del equipo. Evidencia: Configuración de bloqueo automático, políticas de seguridad y resultados de verificaciones.
- Proteger la información institucional que se encuentre en medios físicos o sobre el escritorio, mediante su almacenamiento en cajones, archivadores, espacios restringidos o repositorios seguros cuando no esté siendo utilizada, evitando su exposición, pérdida, copia o acceso por personas no autorizadas. Esta medida debe aplicarse durante toda la jornada laboral y especialmente al finalizar las actividades o abandonar el puesto de trabajo. Evidencia: Verificaciones de escritorio limpio, registros de inspección, reportes de incumplimiento y acciones correctivas.

8.4.9. Supresión de información

Control Asociado en el MSPI A.8.10

Eliminar de forma segura la información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento cuando ya no sea necesaria, con el fin de evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Identificar y eliminar la información asociada a sistemas, aplicaciones y servicios que haya perdido su valor para los procesos de la entidad, mediante la revisión de los inventarios de información y activos y la validación con los responsables de los procesos, cuando se determine su obsolescencia o pérdida de utilidad, dejando como evidencia el inventario actualizado, la autorización de disposición y el registro de eliminación.
- Localizar y eliminar versiones obsoletas, copias no autorizadas y archivos temporales almacenados en equipos, servidores, aplicaciones, repositorios y demás medios bajo administración institucional, mediante revisiones periódicas y actividades de depuración, de acuerdo con los períodos de retención y las necesidades operativas, conservando como evidencia los registros de depuración, reportes de ejecución o logs.
- Ejecutar la eliminación segura y permanente de la información mediante herramientas de borrado seguro previamente evaluadas y autorizadas por la entidad, aplicando métodos que impidan su recuperación mediante herramientas convencionales o técnicas forenses especializadas, antes de la disposición, reutilización, transferencia o reasignación del medio, conservando el registro de la herramienta

utilizada, método aplicado, activo intervenido, fecha, responsable y resultado de la verificación.

- Contratar y utilizar únicamente proveedores autorizados para realizar servicios especializados de eliminación segura, verificando previamente sus certificaciones, capacidades técnicas, condiciones contractuales y mecanismos de trazabilidad, antes de entregarles medios o equipos que contengan información institucional, conservando contratos, certificaciones, órdenes de servicio, actas y certificados de destrucción o eliminación.
- Seleccionar y aplicar el método de eliminación de acuerdo con las características del medio de almacenamiento, su clasificación de información y el nivel de riesgo, utilizando técnicas como borrado seguro, sobreescritura, desmagnetización o destrucción física, según corresponda, antes de su reutilización, disposición o salida de control institucional, registrando el método aplicado y el resultado de la actividad.
- Eliminar la información confidencial y retirar los medios de almacenamiento auxiliares de los equipos que sean devueltos a proveedores, mediante borrado seguro, extracción, destrucción o tratamiento equivalente de discos, memorias y demás componentes que puedan conservar información, antes de que el equipo abandone las instalaciones de la ANCP-CCE, dejando como evidencia el acta de devolución, registro de eliminación y validación técnica correspondiente.
- Seleccionar el mecanismo de eliminación apropiado para dispositivos específicos, evaluando previamente el tipo de dispositivo, la sensibilidad de la información y las capacidades disponibles, utilizando destrucción física o funciones seguras incorporadas, como el restablecimiento a configuración de fábrica cuando resulte técnicamente suficiente, antes

de su entrega, reutilización, transferencia o disposición, conservando el registro del dispositivo, método utilizado y validación de eliminación.

- Destruir físicamente los medios de almacenamiento cuando el nivel de sensibilidad, estado del dispositivo o riesgo de recuperación así lo requiera, mediante procedimientos que inutilicen permanentemente el medio y eviten la recuperación de la información contenida, cuando el borrado lógico no sea suficiente o no pueda garantizarse, conservando actas, certificados, registros fotográficos cuando corresponda y evidencia de disposición final.
- Registrar y formalizar las actividades de eliminación de información, mediante tickets, actas, registros de disposición, certificados de destrucción o herramientas de gestión que permitan identificar como mínimo el activo, información tratada, responsable, método, fecha, motivo y resultado, en cada actividad de eliminación, de manera que la trazabilidad permita reconstruir posteriormente las acciones realizadas y analizar posibles eventos de fuga de información.
- Reportar inmediatamente a Seguridad de la Información cualquier evento o incidente relacionado con pérdida, daño, robo o compromiso de activos de información, así como fallas, errores o incumplimientos detectados durante la eliminación, disposición o reutilización de equipos, utilizando los canales institucionales de gestión de incidentes y suministrando la información y evidencias disponibles, tan pronto como sea identificado el evento, conservando el ticket, reporte, evidencias técnicas y acciones de tratamiento.
- Conservar la información confidencial únicamente durante el período requerido, mediante la aplicación de los períodos de retención definidos en los instrumentos de gestión documental, requisitos legales, regulatorios, contractuales y necesidades del proceso, hasta que se

cumpla la condición que permita su eliminación, manteniendo como evidencia los registros de retención, clasificación, autorización y disposición final.

- Evaluar el mecanismo de eliminación ofrecido por los proveedores de servicios en la nube, verificando sus características técnicas, alcance, garantías de no recuperación, condiciones de eliminación de réplicas, copias de respaldo, almacenamiento temporal y medios asociados, antes de contratar el servicio y cuando se modifiquen las condiciones del proveedor o se requiera retirar información, documentando la evaluación y determinando si el mecanismo institucional es suficiente o si debe solicitarse formalmente al proveedor la eliminación de la información.

8.4.10. Enmascaramiento de datos

Control Asociado en el MSPI A.8.11

Limitar la exposición de datos sensibles, incluida la información personal para cumplir con los requisitos legales, reglamentarios y contractuales por medio del enmascaramiento de datos. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información:

- Definir y recomendar el uso de técnicas de seudonimización o anonimización mediante el análisis de la finalidad del tratamiento, clasificación de los datos, sensibilidad y riesgo de identificación, antes de autorizar el uso de información personal cuando no sea necesario conocer la identidad del titular, documentando la técnica seleccionada, los criterios de aplicación y la evaluación de riesgos.
- Verificar la efectividad de la seudonimización o anonimización mediante pruebas de reidentificación, revisión de identificadores directos e indirectos y análisis de la posibilidad de vincular los datos con otras fuentes, antes de autorizar su utilización y cada vez que cambien la

fuente, estructura, finalidad o técnica aplicada, conservando los resultados de las pruebas y el registro de aprobación.

- Seleccionar y documentar la técnica de enmascaramiento de acuerdo con la clasificación, sensibilidad, finalidad y riesgo de los datos, aplicando mecanismos como cifrado, eliminación o sustitución de caracteres, sustitución de valores, funciones hash u ofuscación, cuando se requiera ocultar total o parcialmente la información original, dejando como evidencia la evaluación, técnica seleccionada y configuración requerida.
- Diseñar consultas, vistas y máscaras de datos aplicando el principio de mínimo privilegio para mostrar únicamente los atributos estrictamente necesarios para la función del usuario, antes de habilitar el acceso a información personal o sensible y cuando cambien los requerimientos de consulta, conservando las consultas, reglas de enmascaramiento, autorizaciones y resultados de las pruebas.
- Establecer condiciones y restricciones para el uso de los datos tratados mediante acuerdos de confidencialidad, controles de acceso, restricciones de copia, descarga, transferencia, correlación y reutilización, antes de suministrar información seudonimizada, anonimizada o enmascarada a funcionarios o terceros, conservando los acuerdos, autorizaciones y registros de acceso.
- Restringir la correlación de los datos tratados con otras fuentes de información mediante controles técnicos y administrativos sobre consultas, cruces, exportaciones y acceso a conjuntos de datos complementarios, durante todo el período en que los datos permanezcan disponibles para tratamiento, verificando periódicamente los controles implementados y conservando registros de acceso, configuraciones y evidencias de monitoreo.
- Realizar seguimiento al suministro y recepción de los datos tratados

mediante el registro de solicitudes, autorizaciones, destinatarios, finalidad, fecha, conjunto de datos suministrado y mecanismo de transferencia, en cada intercambio de información personal seudonimizada, anonimizada o enmascarada, conservando los registros de trazabilidad y evidencias de entrega y recepción.

SIDT:

- Aplicar mecanismos de seudonimización, anonimización o enmascaramiento para ocultar la identidad real de los titulares mediante las técnicas aprobadas por Seguridad de la Información, cuando se identifiquen situaciones de riesgo para la protección de los datos personales o cuando la finalidad del tratamiento no requiera conocer la identidad del titular, dejando como evidencia la configuración aplicada, las pruebas realizadas y el registro de implementación.
- Implementar las consultas, vistas y máscaras de datos definidas por Seguridad de la Información mediante su configuración en bases de datos, aplicaciones y demás repositorios que contengan información personal o sensible, antes de habilitar el acceso y cada vez que se modifiquen los datos, sistemas, permisos o requerimientos de información, conservando las configuraciones, registros de cambio y resultados de las pruebas.
- Implementar mecanismos criptográficos que dificulten los ataques de enumeración sobre los valores reemplazados mediante funciones hash, claves secretas u otros mecanismos criptográficos aprobados, antes de poner en producción el tratamiento basado en hash y durante las revisiones de seguridad correspondientes, conservando la configuración, resultados de pruebas y evidencias de validación.
- Reportar inmediatamente a Seguridad de la Información los eventos o

incidentes relacionados con pérdida, daño, robo o compromiso de activos de información que puedan permitir identificar o establecer la titularidad de información personal, utilizando los canales institucionales de gestión de incidentes, tan pronto como sean detectados, conservando el ticket, registros técnicos, evidencias y acciones de tratamiento.

- Aplicar las técnicas de enmascaramiento definidas y aprobadas por Seguridad de la Información mediante su configuración en los sistemas, bases de datos, aplicaciones y repositorios correspondientes, antes de habilitar el acceso a los datos y cuando se modifique la clasificación, sensibilidad, finalidad o nivel de riesgo, conservando las configuraciones, resultados de las pruebas y registros de implementación.
- Funcionarios y terceros de la entidad deben:
- Reportar inmediatamente a Seguridad de la Información cualquier evento o incidente que pueda permitir la identificación no autorizada de los titulares de información personal, utilizando los canales institucionales establecidos y proporcionando la información disponible sobre el evento, tan pronto como sea detectado, conservando como evidencia el reporte, ticket de incidente y soportes asociados.

8.4.11. Prevención fuga de datos

Control Asociado en el MSPI A.8.12

Detectar e impedir divulgación y extracción no autorizada de información por parte de personas, sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Monitorear los canales institucionales de correo electrónico, transferencia de archivos y dispositivos portátiles de almacenamiento mediante las herramientas de seguridad disponibles, de forma continua

y de acuerdo con los parámetros de monitoreo establecidos, para identificar comportamientos o eventos que puedan indicar fuga o divulgación no autorizada de información. Evidencia: registros de monitoreo, alertas, reportes y casos gestionados.

- Implementar y mantener una herramienta de prevención y detección de fuga de información que permita identificar información sensible, establecer reglas de protección y generar alertas ante intentos de divulgación no autorizada, de acuerdo con la clasificación de la información y los riesgos identificados. Evidencia: herramienta configurada, reglas de protección, reportes y registros de alertas.
- Configurar y aplicar mecanismos de bloqueo o restricción sobre las acciones de los usuarios y las transmisiones de red que impliquen riesgo de exposición de información confidencial, cuando se detecten eventos que incumplan las reglas de protección definidas. Evidencia: reglas de bloqueo, registros de eventos y reportes de incidentes.
- Evaluar y documentar los casos en los que sea necesario restringir la capacidad de determinados usuarios para copiar, pegar, cargar o transferir información hacia servicios, dispositivos o medios de almacenamiento externos, considerando la clasificación de la información, el perfil del usuario y el nivel de riesgo. Evidencia: análisis de riesgo, matriz de restricciones y autorizaciones.
- Solicitar y validar la autorización del propietario de la información antes de permitir la exportación, copia o transferencia de información clasificada como sensible, confidencial o restringida, cuando la actividad se encuentre fuera de los usos autorizados. Evidencia: solicitud y autorización registrada.
- Definir, publicar y comunicar los términos y condiciones para la captura de evidencias mediante capturas de pantalla o fotografías de pantalla,

estableciendo previamente las restricciones relacionadas con información personal, confidencial, sensible o clasificada. Evidencia: lineamiento publicado, registro de divulgación y material de sensibilización.

- Monitorear el uso y movimiento de información mediante los controles tecnológicos disponibles y generar alertas cuando se identifiquen comportamientos asociados con riesgo de fuga de información; aplicar medidas preventivas o de bloqueo, según el nivel de riesgo, incluyendo la restricción de transferencias hacia dispositivos portátiles de almacenamiento externo. Evidencia: alertas, registros de eventos, bloqueos efectuados e informes de seguimiento.

La SIDT

- Configurar y utilizar FALCON para monitorear los eventos relacionados con información sensible y posibles mecanismos de divulgación no autorizada mediante servicios, dispositivos o medios de almacenamiento externos, de acuerdo con las capacidades habilitadas de la solución y las reglas de seguridad definidas. Evidencia: políticas configuradas, alertas, eventos registrados y reportes de FALCON.
- Aplicar cifrado, controles de acceso y medidas de protección física sobre los medios de almacenamiento que contengan copias de seguridad con información sensible o datos personales, desde su generación hasta su eliminación o destrucción segura, restringiendo el acceso exclusivamente al personal autorizado. Evidencia: configuración de cifrado, registros de acceso, inventario de medios y controles de custodia.

Los funcionarios y terceros de la entidad

- Consultar y aplicar los términos y condiciones establecidos para la captura de evidencias mediante capturas de pantalla, antes de realizar la captura y durante su almacenamiento o transferencia, evitando incluir información que no sea necesaria para la evidencia. Evidencia: capturas realizadas conforme al lineamiento y registros de cumplimiento cuando aplique.
- Reportar a Seguridad de la Información, mediante los canales institucionales definidos y tan pronto como tengan conocimiento del evento, cualquier situación que implique pérdida, daño, robo, acceso no autorizado o compromiso de activos de información relacionado con una posible fuga o exposición de información personal. Evidencia: ticket, reporte de incidente o registro de la notificación.
- Identificar y clasificar la información que creen, reciban, procesen, almacenen o compartan, aplicando los criterios de clasificación establecidos por la entidad y antes de realizar su almacenamiento, transferencia o divulgación, con el fin de determinar los controles de protección requeridos. Evidencia: información clasificada, registros de inventario y mecanismos de etiquetado

8.4.12. Información de prueba

Control Asociado en el MSPI A.8.33

Realizar la selección, protección y control de los datos utilizados en las pruebas de los sistemas de información y efectuarlas de manera cuidadosa. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Solicitar y validar la autorización del usuario funcional responsable de la información antes de copiar cualquier información operacional desde el

ambiente de producción hacia los ambientes de desarrollo y/o pruebas, cada vez que se requiera realizar dicha copia y antes de efectuarla, verificando que la solicitud identifique como mínimo la información a copiar, finalidad, ambiente destino, período de utilización y responsable. Evidencia: solicitud y autorización registrada.

- Realizar la copia de información operacional hacia los ambientes de desarrollo y/o pruebas únicamente después de contar con la autorización correspondiente, utilizando mecanismos controlados de transferencia y aplicando las medidas de protección definidas para la información. Evidencia: registros de transferencia, bitácoras de acceso y autorización asociada.
- Eliminar de forma segura la información operacional copiada en los ambientes de desarrollo y/o pruebas una vez finalizadas las pruebas o cuando deje de ser necesaria, sin conservar copias adicionales no autorizadas, verificando posteriormente que la información haya sido eliminada de los repositorios utilizados. Evidencia: registro de eliminación, bitácora del sistema y evidencia de verificación.
- Registrar las actividades de copia, acceso, utilización y eliminación de información operacional mediante los mecanismos de trazabilidad disponibles, durante todo el período autorizado de utilización y cuando se requiera efectuar auditorías o investigaciones, conservando los registros de acuerdo con los tiempos de retención establecidos. Evidencia: logs, bitácoras, tickets, reportes de auditoría y registros de trazabilidad.
- Verificar que la información confidencial de los ambientes de producción no sea expuesta en los ambientes de desarrollo y/o pruebas, mediante la revisión de los datos utilizados, configuraciones de acceso y resultados de las pruebas, antes de habilitar el ambiente para su utilización y

durante las revisiones periódicas establecidas. Evidencia: listas de verificación, actas o registros de revisión y resultados de las validaciones.

- Evitar el uso de información personal o sensible proveniente de producción en ambientes de desarrollo y/o pruebas, mediante la utilización de datos ficticios, sintéticos o anonimizados; cuando excepcionalmente sea necesario utilizar datos reales, aplicar previamente técnicas de anonimización o enmascaramiento que impidan identificar a las personas o recuperar la información original, de acuerdo con los controles definidos. Evidencia: datos anonimizados/enmascarados, procedimiento aplicado y registro de validación.
- Aplicar controles de acceso diferenciados para los ambientes de producción, desarrollo y pruebas, utilizando cuentas individuales, perfiles basados en roles y privilegios mínimos, desde la habilitación del acceso y durante todo el período en que este se encuentre autorizado, revisando y retirando los permisos cuando ya no sean necesarios. Evidencia: matriz de accesos, solicitudes y aprobaciones, registros de autenticación y revisiones periódicas de privilegios.
- Enmascarar la información utilizada en las pruebas mediante técnicas que sustituyan, oculten o transformen los datos sensibles o confidenciales, antes de su entrega o utilización en el ambiente de desarrollo y/o pruebas, verificando que el proceso no permita recuperar o inferir la información original cuando esto no esté autorizado. Evidencia: configuración de enmascaramiento, muestras de datos transformados y registro de validación.
- Certificar la no divulgación de información confidencial de producción mediante una validación previa y posterior a las pruebas, verificando que

los datos utilizados, resultados, archivos temporales, registros y evidencias generadas no contengan información confidencial de producción que no haya sido expresamente autorizada. Responsable: SIDT, con participación del usuario funcional o propietario de la información cuando corresponda. Evidencia: certificación de revisión, lista de verificación y registros de eliminación o corrección de hallazgos.

8.4.13. Protección de sistemas de información durante pruebas de auditoría (8.34)

Control Asociado en el MSPI A.8.34

Minimizar impacto de auditorías y otras actividades de garantía en los sistemas operativos y los procesos empresariales. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Definir los requisitos de auditoría para acceso a sistemas y datos y mecanismo de solicitud.
- Ofrecer el acceso al software y datos únicamente sea en modo de lectura para los procesos de auditoría.
- Otorgar acceso de solo lectura a los archivos file systems y si se requiere un acceso diferente se debe proveer copias aisladas, las cuales serán borradas una vez terminada la visita.
- Definir el alcance de las pruebas técnicas y los requisitos para solicitudes especiales y hacer el seguimiento de estas.
- Llevar a cabo el procedimiento de cambios las pruebas de auditoría en producción que se vayan a realizar.
- Verificar que las pruebas de auditoría en producción se realicen fuera del horario laboral, para evitar la indisponibilidad o lentitud de los sistemas de información y afectación de los servicios.
- Revisar logs para las operaciones de la auditoría.

- Establecer la relación de responsabilidades que tienen los usuarios que tengan acceso a los logs de auditoría.
- Incluir protocolos de autenticación en la red para los usuarios que tengan acceso a los logs de auditoría.
- Fortalecer la seguridad y optimizar los dispositivos de red y los controles asociados cuando un usuario realice acceso a los logs de auditoría de los sistemas.
- Validar y, si es necesario, aislar temporalmente subredes críticas para los procesos de auditoría de los sistemas.
- Deshabilitar protocolos de red vulnerables para el acceso a los logs de auditoría de los sistemas, esta actividad se debe realizar en toda la red.

La Oficina de Control Interno:

- Solicitar a la SIDT los accesos de solo lectura a los sistemas operativos que desee hacer auditoria de los sistemas dentro del plan de auditoría que disponga para el año.
- Indicar a la SIDT los tiempos requeridos de accesos a los logs de auditoría. En caso de que se vayan a utilizar herramientas para este propósito, se debe notificar y planificar su ejecución; las herramientas no pueden afectar el funcionamiento de los sistemas.
- Hacer uso adecuado y bajo las condiciones que indique la SIDT de los accesos que sean otorgados en los sistemas.

8.5. Componente Política de Control de acceso

8.5.1. Acceso a la información

Control Asociado en el MSPI A.5.15

Restringir el acceso a la información, sistemas de información y aplicaciones únicamente a personal autorizado, de acuerdo con la política de control de acceso establecida en este manual. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Asignar y segmentar los privilegios de acceso de los usuarios mediante roles y perfiles de seguridad, aplicando el principio de mínimo privilegio y otorgando únicamente los permisos requeridos para las funciones autorizadas. Realizar la asignación y revisión de privilegios durante el alta, modificación o retiro de usuarios y periódicamente según la frecuencia establecida. Evidencia: matriz de roles y permisos, solicitudes de acceso, aprobaciones y registros de revisión.
- Verificar la aplicación de los lineamientos de seguridad para el acceso a información electrónica, mediante la revisión de los permisos asignados, controles de autenticación, restricciones de transferencia y mecanismos de protección definidos para cada nivel de clasificación de información. Realizar la verificación durante la habilitación del acceso y en las revisiones periódicas de los sistemas. Evidencia: listas de verificación, matrices de acceso, configuraciones de seguridad y reportes de revisión.
- Impedir el acceso a información sensible mediante identidades no identificadas, genéricas o no autorizadas, utilizando mecanismos de autenticación individual, validación de identidad y autorización basada en roles. Bloquear o revocar inmediatamente las credenciales que no puedan ser asociadas con un usuario autorizado o que presenten condiciones de riesgo. Evidencia: registros de autenticación, eventos de bloqueo, inventario de cuentas y reportes de revisión.
- Implementar mecanismos técnicos para controlar el acceso a la información, mediante autenticación, autorización, perfiles de usuario, control de privilegios, segmentación y registro de eventos, de acuerdo con la criticidad del sistema y clasificación de la información protegida. Revisar periódicamente la efectividad de estos mecanismos. Evidencia:

configuraciones de seguridad, políticas de acceso, registros de eventos y resultados de las revisiones.

- Controlar los datos y recursos a los que puede acceder cada usuario, mediante la aplicación del procedimiento CCE-GTI-PR-O4 Procedimiento Infraestructura y asignación de cuentas y el diligenciamiento del formato CCE-GTI-FM-60, verificando que el acceso solicitado corresponda a las funciones y responsabilidades del usuario. Aplicar el control durante el alta, modificación, cambio de funciones y retiro del usuario. Evidencia: formato CCE-GTI-FM-60, solicitudes, aprobaciones y registros de configuración.
- Gestionar las identidades y grupos autorizados para acceder a los sistemas de información, mediante directorios institucionales, grupos de seguridad y mecanismos centralizados de administración de identidades, manteniendo actualizada la relación de usuarios y grupos autorizados y retirando oportunamente las cuentas que pierdan su condición de autorización. Evidencia: inventario de cuentas y grupos, registros de altas/bajas y reportes de revisión de accesos.
- Implementar controles de acceso lógico sobre los sistemas de información, mediante autenticación individual, políticas de contraseñas, MFA cuando corresponda, autorización por roles, mínimo privilegio, bloqueo de sesiones y registro de actividades, de acuerdo con la criticidad y nivel de exposición de cada sistema. Evidencia: políticas configuradas, parámetros de seguridad, registros de autenticación y reportes de monitoreo.
- Identificar los sistemas de información que procesan o almacenan información sensible, mediante la revisión del inventario de activos y su relación con los niveles de clasificación de información, actualizando esta identificación cuando se incorporen, modifiquen o retiren sistemas o

cuando cambie la clasificación de la información. Evidencia: inventario de activos, matriz de clasificación y registro de actualización.

- Implementar ambientes tecnológicos aislados e independientes para los sistemas que procesen información sensible, mediante segmentación de redes, controles de firewall, separación de ambientes, restricciones de comunicación y controles de acceso específicos, cuando el análisis de riesgo y la clasificación de la información determinen la necesidad de aislamiento. Evidencia: diagramas de arquitectura, reglas de firewall, configuraciones de segmentación y análisis de riesgo.
- Aislar los sistemas que procesen información sensible de fuentes de datos no autorizadas, mediante controles de segmentación lógica, reglas de comunicación, listas de acceso y restricciones de conexión entre ambientes, permitiendo únicamente las comunicaciones requeridas para la operación y previamente autorizadas. Revisar periódicamente las reglas para eliminar accesos o comunicaciones que ya no sean necesarios. Evidencia: reglas de firewall, ACL, configuraciones de red, diagramas de segmentación y registros de revisión.

Gestión Administrativa

- Restringir el acceso físico a información clasificada, mediante controles de acceso a áreas, archivadores, depósitos y demás espacios donde se almacene o consulte información física, aplicando niveles de restricción de acuerdo con la clasificación de la información y autorizando únicamente al personal que requiera acceso para el cumplimiento de sus funciones. Revisar y actualizar periódicamente las autorizaciones y retirarlas cuando cambien las funciones o finalice la necesidad de acceso. Evidencia: registros de acceso físico, autorizaciones, inventarios, controles de custodia y actas de revisión.

8.5.2. Gestión de identidad

Control Asociado en el MSPI A.5.16

Proporcionar gestión y control seguros de las identidades digitales a lo largo de su ciclo de vida. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Definir y mantener los lineamientos y controles para la gestión de identidades mediante reglas documentadas para el ciclo de vida de las cuentas —creación, modificación, suspensión, bloqueo y eliminación—, asignación de roles, autenticación, gestión de privilegios y revisión de accesos. Revisar periódicamente su aplicación y actualizar los controles cuando se presenten cambios tecnológicos, organizacionales, normativos o de riesgo. Evidencia: lineamientos aprobados, matriz de controles, registros de revisión y reportes de seguimiento.
- Monitorear las identidades y los accesos asignados a funcionarios y terceros mediante la revisión de las cuentas activas, roles, privilegios y registros de autenticación, de acuerdo con la periodicidad establecida y ante cambios de cargo, desvinculación, incidentes o detección de accesos anómalos. Evidencia: reportes de revisión, inventario de identidades, registros de autenticación y hallazgos gestionados.

La SIDT

- Implementar los lineamientos y controles de gestión de identidades definidos por Seguridad de la Información, mediante la configuración de políticas de autenticación, administración de cuentas, asignación de roles, control de privilegios y trazabilidad de accesos, de acuerdo con los requisitos institucionales y cada vez que se incorporen o modifiquen sistemas de información. Evidencia: configuraciones, políticas aplicadas,

registros de implementación y resultados de las verificaciones.

- Asignar una cuenta individual y un identificador único a cada funcionario y tercero autorizado, mediante el directorio institucional o la solución de gestión de identidades adoptada, antes de habilitar el acceso a los sistemas de información y evitando el uso compartido de cuentas personales. Evidencia: directorio de usuarios, solicitud y aprobación de cuenta, inventario de identidades y registros de autenticación.
- Restringir el uso de cuentas con privilegios de administrador local en los equipos de usuario, mediante la eliminación, deshabilitación o control de dichas cuentas y la utilización de mecanismos de elevación de privilegios administrados por la SIDT, permitiendo su utilización únicamente cuando sea necesaria para actividades autorizadas de soporte técnico. Evidencia: configuración de equipos, políticas de privilegios, registros de elevación y tickets de soporte.
- Verificar que las aplicaciones y sistemas de información utilicen mecanismos de autenticación integrados con las identidades institucionales administradas por el controlador de dominio o por la solución corporativa de gestión de identidades, antes de su puesta en producción y durante las revisiones de seguridad o modificaciones relevantes, documentando las excepciones técnicamente justificadas. Evidencia: inventario de sistemas, configuraciones de autenticación, documentación técnica y registros de verificación.
- Asignar roles y privilegios a los usuarios internos mediante solicitudes formales de acceso, verificando previamente que el rol requerido corresponda con las funciones del usuario y cuente con la aprobación de su jefe inmediato o responsable autorizado. Aplicar el mismo mecanismo ante modificaciones o ampliaciones de privilegios. Evidencia: solicitud de acceso, aprobación, matriz de roles y registro de asignación.

- Gestionar el ciclo de vida de las identidades mediante el controlador de dominio o la solución tecnológica institucional de gestión de identidades, centralizando la creación, modificación, suspensión, bloqueo y eliminación de cuentas y aplicando los controles de autenticación y autorización definidos. Ejecutar las modificaciones cuando se produzcan altas, cambios de funciones, transferencias, suspensiones o desvinculaciones. Evidencia: registros del sistema de gestión de identidades, bitácoras de cambios, solicitudes y reportes de cuentas activas.

Los funcionarios y terceros

- Actualizar las credenciales de acceso de acuerdo con las políticas institucionales de autenticación, utilizando mecanismos seguros de cambio de contraseña y realizando el cambio cuando sea requerido por la política, ante sospecha o evidencia de compromiso, restablecimiento de credenciales o solicitud de la SIDT. Evidencia: registros de cambio o restablecimiento de credenciales generados por el sistema.
- Aplicar los lineamientos de gestión de identidades establecidos por la entidad, utilizando exclusivamente las cuentas, roles y mecanismos de autenticación autorizados y atendiendo las instrucciones relacionadas con creación, modificación, protección y uso de las credenciales. Evidencia: registros de aceptación, capacitaciones, campañas de sensibilización y resultados de revisiones o auditorías.
- Utilizar exclusivamente la identidad y contraseña asignadas de manera individual, manteniendo las credenciales bajo custodia personal, sin compartirlas, almacenarlas de forma insegura ni permitir su utilización por terceros. Reportar inmediatamente a la SIDT cualquier sospecha de pérdida, divulgación o compromiso de las credenciales. Evidencia:

registros de autenticación, reportes de incidentes y tickets de atención.

- Reportar los roles, permisos o privilegios que no sean necesarios para el cumplimiento de las funciones asignadas, mediante los canales institucionales definidos, tan pronto como sean identificados y especialmente cuando se produzcan cambios de cargo, responsabilidades o funciones. Evidencia: solicitud o ticket de reporte, registro de modificación o revocación del privilegio y confirmación de cierre.

8.5.3. Información de autenticación

Control Asociado en el MSPI A.5.17

Proteger la información usada para la autenticación contra su uso o divulgación no autorizada. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Establecer y mantener un proceso para la asignación, entrega, sustitución, recuperación y revocación de información de autenticación, mediante procedimientos documentados que definan la validación de identidad, responsables, mecanismos de entrega, requisitos de contraseña, tratamiento de credenciales provisionales y controles para cuentas privilegiadas. Aplicar el proceso cada vez que se cree, modifique, sustituya, desbloquee o retire una cuenta. Evidencia: procedimiento aprobado, solicitudes, registros de asignación y bitácoras.
- Gestionar el cambio de contraseña únicamente mediante solicitudes realizadas por el titular de la cuenta o, excepcionalmente, por su jefe o supervisor inmediato, cuando el titular no disponga de los medios técnicos para realizarlo. Validar la identidad y autorización del solicitante antes de ejecutar el cambio. Evidencia: solicitud, validación de identidad y registro del cambio.

- Configurar las políticas de contraseñas de los sistemas de información estableciendo una longitud mínima y, cuando técnicamente corresponda, una longitud máxima, de acuerdo con las capacidades de cada plataforma y el nivel de riesgo del sistema. Revisar estos parámetros cuando se incorporen nuevos sistemas o se actualicen los mecanismos de autenticación. Evidencia: políticas de contraseña, parámetros configurados y resultados de verificación.
- Configurar requisitos de complejidad para las contraseñas, mediante la combinación de los tipos de caracteres permitidos por la solución institucional —mayúsculas, minúsculas, números y caracteres especiales— y evitando patrones fácilmente predecibles. Aplicar estos requisitos durante la creación y modificación de las credenciales. Evidencia: configuración de políticas y pruebas de cumplimiento.
- Aplicar requisitos reforzados de autenticación para administradores y cuentas privilegiadas, mediante contraseñas robustas, autenticación multifactor cuando esté disponible, cuentas individuales y controles adicionales de monitoreo y trazabilidad. Aplicar estos controles antes de otorgar privilegios administrativos y durante las revisiones periódicas de dichas cuentas. Evidencia: inventario de cuentas privilegiadas, configuración MFA, matriz de privilegios y registros de autenticación.
- Impedir el reúso de contraseñas mediante la configuración del historial de credenciales en los sistemas que lo permitan, manteniendo un historial que evite reutilizar las contraseñas anteriores conforme a la política institucional. Aplicar el control durante cada cambio de contraseña. Evidencia: configuración de políticas y registros de validación.
- Evitar la transmisión de contraseñas mediante correo electrónico, utilizando mecanismos controlados de generación, restablecimiento o

entrega de credenciales que no expongan la contraseña en texto claro. Aplicar esta restricción durante la creación, recuperación y sustitución de credenciales. Evidencia: configuración del mecanismo de autenticación, procedimiento de recuperación y registros de servicio.

- Definir y mantener lineamientos para atender los requerimientos relacionados con la información de autenticación, estableciendo mecanismos de solicitud, validación de identidad, aprobación, asignación, recuperación, bloqueo, desbloqueo, cambio y revocación. Revisar los lineamientos periódicamente y cuando se presenten cambios tecnológicos, normativos o de riesgo. Evidencia: lineamientos aprobados, registros de revisión y actualizaciones.
- Promover buenas prácticas para la protección de la información de autenticación, mediante campañas de sensibilización, capacitación y comunicaciones institucionales que instruyan sobre la creación y protección de contraseñas, prohibición de compartir credenciales, identificación de intentos de phishing y reporte de compromisos. Realizar las actividades de acuerdo con el programa de sensibilización establecido. Evidencia: material de capacitación, registros de asistencia, campañas y evaluaciones.

La SIDT

- Implementar los lineamientos y controles de autenticación definidos por Seguridad de la Información, mediante la configuración de las políticas de contraseñas, mecanismos de autenticación, gestión de cuentas, recuperación de credenciales y controles para cuentas privilegiadas. Verificar su aplicación durante la implementación de los sistemas y en las revisiones periódicas de seguridad. Evidencia: configuraciones, políticas aplicadas, reportes de verificación y registros de auditoría.

- Verificar la identidad del usuario antes de asignar, sustituir, restablecer o entregar información de autenticación, utilizando mecanismos de validación definidos por la entidad y diferenciando los procedimientos según el nivel de privilegio de la cuenta. Aplicar la validación en cada solicitud de creación, recuperación o sustitución de credenciales. Evidencia: solicitud, registro de validación y ticket de atención.
- Suministrar los mecanismos de autenticación mediante canales institucionales seguros, evitando enviar contraseñas en texto claro por correo electrónico o por medios no autorizados; cuando se requiera comunicación al usuario, utilizar mecanismos de activación o restablecimiento que permitan establecer la contraseña directamente por el titular. Evidencia: registros de entrega, activación o restablecimiento de credenciales.
- Implementar y administrar una solución institucional para la gestión de contraseñas, configurando los parámetros de longitud, complejidad, historial, bloqueo, expiración, recuperación y demás controles definidos por la entidad, de acuerdo con las capacidades del sistema y el nivel de riesgo asociado. Evidencia: configuración de la herramienta, políticas aplicadas y reportes de cumplimiento.
- Validar periódicamente la vigencia de las autorizaciones de acceso de los usuarios externos, mediante la revisión de la relación de usuarios, responsables, fechas de vencimiento y necesidad de acceso. Solicitar la renovación antes del vencimiento y bloquear las cuentas cuya autorización no sea renovada; eliminar las cuentas que permanezcan bloqueadas durante tres meses, previa validación de que no exista una necesidad vigente de conservación. Evidencia: matriz de usuarios externos, solicitudes de renovación, registros de bloqueo y eliminación.
- Forzar el cambio de contraseña en el primer inicio de sesión de los

usuarios nuevos, mediante la configuración de la política de autenticación del sistema para impedir el uso continuado de credenciales provisionales. Aplicar adicionalmente el cambio cuando exista compromiso de credenciales, recuperación de cuenta, evento de seguridad o condición definida por la política institucional. Evidencia: configuración de política y registros de cambio de contraseña.

- Aplicar los mecanismos de autenticación segura durante el desarrollo o adquisición de sistemas de información, incorporando requisitos de autenticación, gestión de sesiones, protección de credenciales, control de intentos fallidos, MFA cuando corresponda y gestión segura de contraseñas desde las etapas de diseño y pruebas. Verificar su cumplimiento antes de la puesta en producción. Evidencia: requisitos de seguridad, resultados de pruebas, documentación técnica y acta de validación.

Los funcionarios y terceros de la entidad

- Formalizar el compromiso de confidencialidad antes de recibir o utilizar credenciales de acceso, mediante la aceptación de los instrumentos institucionales definidos para la protección de la información y las credenciales. Mantener vigente el compromiso durante todo el período de vinculación y acceso a los sistemas. Evidencia: compromiso de confidencialidad suscrito o registro de aceptación.
- Aplicar los instructivos institucionales para la creación, activación, uso, protección, recuperación y cambio de las cuentas de usuario, siguiendo los mecanismos y requisitos definidos por la ANCP-CCE y reportando inmediatamente cualquier pérdida, divulgación, uso indebido o sospecha de compromiso de las credenciales. Evidencia: registros de aceptación, solicitudes, tickets de soporte y reportes de incidentes.

8.5.4. Derechos de acceso

Control Asociado en el MSPI A.5.18

Asegurar que los derechos de acceso estén alineados con las funciones del usuario y sean revisados periódicamente. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Gestionar la integración de los sistemas de información con las plataformas institucionales de seguridad, mediante la instalación, configuración y validación de agentes o conectores para el envío de eventos de autenticación, cambios, reinstalaciones y actividades relevantes hacia el SIEM, así como para la protección de bases de datos y la gestión de identidades centralizadas y privilegiadas. Realizar la integración durante la incorporación de nuevos sistemas, modificaciones relevantes o reinstalaciones y verificar su funcionamiento posteriormente. Evidencia: inventario de sistemas integrados, configuración de agentes, registros del SIEM y resultados de pruebas de integración.
- Centralizar la gestión de identidades y roles de acceso mediante el controlador de dominio o la solución institucional de gestión de identidades, asociando los permisos a las funciones y responsabilidades de cada usuario. Aplicar esta gestión durante la creación, modificación, traslado o retiro de usuarios y revisar periódicamente los privilegios asignados. Evidencia: directorio de identidades, matriz de roles, solicitudes y aprobaciones de acceso.
- Gestionar oportunamente la desactivación, suspensión, modificación o revocación de los privilegios de acceso mediante el procedimiento institucional de gestión de identidades, activando las acciones correspondientes cuando se presenten desvinculaciones, licencias,

vacaciones, incapacidades, permisos, traslados, cambios de dependencia, cambios de cargo o proceso, sanciones disciplinarias o terminación de contratos. Evidencia: notificación de novedad, solicitud de modificación y registros de inactivación o revocación.

- Notificar al usuario las modificaciones o inactivaciones de sus accesos, mediante los canales institucionales definidos, cuando la condición administrativa permita dicha comunicación y de acuerdo con las restricciones de seguridad aplicables, dejando constancia de la notificación cuando corresponda. Evidencia: correo, ticket, comunicación formal o registro de notificación.

La SIDT

- Registrar y mantener actualizado el inventario de cuentas con privilegios elevados, identificando las cuentas de superusuario, administrador, servicio y demás cuentas con permisos especiales en cada sistema de información. Actualizar el registro cuando se creen, modifiquen, suspendan o eliminen cuentas privilegiadas y monitorear permanentemente sus actividades. Evidencia: inventario de cuentas privilegiadas, matriz de permisos y registros de monitoreo.
- Integrar los sistemas de información al controlador de dominio o solución centralizada de identidades, mediante mecanismos de autenticación compatibles y configuraciones de confianza o federación cuando corresponda, priorizando los sistemas que procesen información crítica o sensible y verificando la integración antes de habilitar el acceso de los usuarios. Evidencia: configuraciones de integración, pruebas de autenticación, inventario de sistemas integrados y registros de acceso.
- Clasificar los tipos de usuarios y perfiles de acceso mediante una matriz de roles, relacionando las funciones de la dependencia, el tipo de

información requerida y las acciones permitidas sobre dicha información. Revisar la matriz cuando cambien las funciones, procesos, sistemas o niveles de clasificación de la información. Evidencia: matriz de roles y permisos, aprobaciones y registros de actualización.

- Gestionar la creación, modificación, suspensión y eliminación de cuentas mediante un procedimiento formal de gestión de accesos, estableciendo el solicitante, responsable de aprobación, nivel de acceso requerido, vigencia y mecanismo de implementación. Aplicar el procedimiento en cada alta, cambio de funciones, traslado, retiro o modificación de privilegios. Evidencia: solicitudes, aprobaciones, tickets y registros de cambios.
- Generar reportes de acceso y uso de los sistemas de información mediante los mecanismos de auditoría y monitoreo disponibles, proporcionando a los responsables de las dependencias la información necesaria para verificar que los accesos correspondan con las funciones autorizadas. Realizar la generación y entrega de reportes de acuerdo con la periodicidad establecida o cuando sea requerida una revisión extraordinaria. Evidencia: reportes de acceso, registros de actividad y constancias de revisión.
- Mantener actualizado el inventario de cuentas y permisos administrativos de los recursos tecnológicos, mediante la comparación entre las cuentas existentes, los responsables autorizados y las funciones vigentes. Realizar como mínimo dos revisiones al año y adicionalmente cuando se presenten cambios organizacionales, incidentes o modificaciones relevantes. Evidencia: inventario actualizado, matriz de privilegios, actas o informes de revisión y registros de depuración.
- Inactivar los derechos de acceso mediante la herramienta institucional

de gestión de identidades cuando un usuario se encuentre en vacaciones, incapacidad, licencia, permiso, suspensión disciplinaria u otra ausencia temporal que requiera la restricción del acceso. Reactivar los permisos únicamente mediante solicitud del jefe inmediato y previa validación de la necesidad; ante la desvinculación o terminación de la relación contractual, revocar definitivamente los accesos. Evidencia: solicitud de inactivación/reactivación, aprobación y registros de la herramienta de gestión de identidades.

- Gestionar el acceso de usuarios con roles sensibles mediante una solución de Gestión de Identidades Privilegiadas (PIM/PAM), utilizando cuentas individuales, autorización previa, asignación temporal de privilegios cuando sea posible, trazabilidad de las sesiones y registro de las actividades realizadas. Aplicar estos controles a superusuarios, administradores y usuarios que ejecuten transacciones críticas. Evidencia: registros de sesiones privilegiadas, autorizaciones, trazabilidad y reportes de la herramienta PAM/PIM.
- Verificar que las aplicaciones y sistemas de información utilicen cuentas administradas por el controlador de dominio o por la solución corporativa de identidades, mediante revisiones de configuración y pruebas de autenticación. Realizar la verificación antes de la puesta en producción y durante las revisiones periódicas o modificaciones relevantes, documentando las excepciones justificadas. Evidencia: resultados de pruebas, configuraciones, inventario de aplicaciones y documentación de gestión de identidades.
- Monitorear las cuentas de usuarios, superusuarios, administradores, cuentas genéricas y cuentas de servicio con privilegios especiales, mediante los registros de autenticación, SIEM, herramientas de gestión de identidades y mecanismos de detección disponibles. Realizar el

monitoreo de forma continua para cuentas privilegiadas y de acuerdo con la capacidad de las herramientas para las demás cuentas. Evidencia: logs, alertas, reportes de monitoreo y casos gestionados.

- Identificar y eliminar cuentas genéricas, duplicadas o adicionales con privilegios administrativos que no tengan una justificación vigente, mediante revisiones del inventario de identidades y validación con los responsables de los sistemas. Realizar la eliminación o deshabilitación después de confirmar que la cuenta no sea requerida para una operación legítima, servicio o proceso autorizado. Evidencia: inventario depurado, aprobación de eliminación y registros de inactivación.

Funcionarios y terceros de la entidad

- Reportar las novedades que puedan generar la modificación, suspensión o retiro de los derechos de acceso, mediante los canales institucionales establecidos, tan pronto como se produzca o sea conocida la novedad, indicando el usuario, tipo de novedad, fecha efectiva y sistemas afectados cuando corresponda. Evidencia: solicitud, ticket, correo institucional o registro de novedad.
- Jefes de las dependencias
- Verificar que los usuarios bajo su responsabilidad mantengan únicamente los roles y privilegios necesarios para ejecutar sus funciones, mediante la revisión de la matriz de accesos y los reportes suministrados por la SIDT, de acuerdo con el procedimiento PR-IIT-0455, Gestión de Accesos, y en las revisiones periódicas establecidas. Evidencia: validación de accesos, aprobación de roles y registros de revisión.
- Validar periódicamente los roles asignados a los usuarios de su dependencia, comparándolos con las funciones actuales y solicitando la modificación o inactivación de los accesos que no estén justificados.

Realizar la solicitud inmediatamente cuando se detecte un acceso no autorizado o innecesario. Evidencia: reporte de revisión, solicitudes de modificación y registros de inactivación.

- Depurar los roles y privilegios asignados a los usuarios, mediante la identificación de permisos que hayan perdido su justificación por cambios de funciones, traslado, retiro o modificación de responsabilidades. Solicitar oportunamente la revocación de los accesos que ya no sean necesarios, incluidos los accesos a sistemas externos. Evidencia: matriz actualizada, solicitudes de revocación y confirmación de cierre.
- Reportar oportunamente las novedades de desvinculación, traslado o cambio de rol de funcionarios y terceros, mediante los canales institucionales establecidos y antes o inmediatamente después de que la novedad sea efectiva, según el procedimiento aplicable, para permitir a la SIDT ejecutar las acciones de modificación o revocación de accesos. Evidencia: comunicación oficial, ticket, registro de Gestión Administrativa y confirmación de cierre por parte de la SIDT.

8.5.5. Derechos de acceso privilegiado

Control Asociado en el MSPI A.8.2

Restringir y controlar los accesos privilegiados, para la asignación y uso de derechos de acceso a los diferentes programas, servicios, aplicativos, bases de datos y cualquier acceso a actividades específicas de la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT:

- Gestionar las solicitudes de acceso privilegiado mediante un procedimiento formal que establezca la justificación del acceso, sistema o recurso requerido, nivel de privilegio, tiempo de vigencia, responsable de aprobación y condiciones de uso; aplicarlo en cada alta, modificación

o renovación de privilegios y revisarlo periódicamente conforme a la política de control de acceso. Evidencia: procedimiento aprobado, solicitudes, autorizaciones y registros de acceso.

- Validar y asignar los privilegios de administración mediante la verificación previa del cargo, funciones, competencias técnicas y necesidad de acceso del funcionario, requiriendo aprobación del responsable autorizado antes de habilitar la cuenta; realizar esta validación en cada solicitud de acceso o modificación de privilegios. Evidencia: matriz de roles y privilegios, solicitud aprobada, registros de aprovisionamiento y cuenta asignada.
- Registrar y actualizar los accesos privilegiados mediante un inventario centralizado que identifique funcionario, cuenta, sistema, recurso, nivel de privilegio, responsable de autorización, fecha de asignación y vigencia; actualizarlo cada vez que se otorgue, modifique o revoque un privilegio y verificarlo periódicamente. Evidencia: inventario de cuentas privilegiadas, historial de cambios y actas o informes de revisión.
- Restringir la instalación de programas y modificaciones de configuración con capacidad de escalamiento de privilegios mediante políticas de control de aplicaciones, administración centralizada de estaciones, perfiles sin privilegios administrativos y listas de aplicaciones autorizadas; aplicar estos controles de forma permanente y revisar las excepciones mediante autorización formal. Evidencia: políticas de configuración, registros de bloqueo, inventario de software, excepciones autorizadas y reportes de monitoreo.
- Gestionar el uso de programas utilitarios privilegiados mediante un catálogo aprobado de herramientas autorizadas para la administración de la plataforma, validando su necesidad, origen, versión y responsable de uso; revisar y actualizar el catálogo periódicamente y retirar o

deshabilitar las herramientas no autorizadas cuando sean identificadas. Evidencia: catálogo aprobado, registros de revisión, inventario de software, tickets de desinstalación/deshabilitación y evidencias de socialización.

- Restringir las conexiones remotas a los recursos tecnológicos mediante VPN, listas de control de acceso, autenticación individual y mecanismos de autenticación reforzada cuando estén disponibles, permitiendo únicamente las conexiones provenientes de usuarios, dispositivos y ubicaciones autorizadas; revisar los accesos y registros de conexión de acuerdo con el nivel de criticidad del recurso. Evidencia: configuraciones de VPN/firewall, reglas de acceso, registros de autenticación y reportes de conexiones remotas.
- Deshabilitar temporalmente los servicios, cuentas o funcionalidades asociadas a usuarios que se encuentren retirados temporalmente de sus funciones mediante los mecanismos centralizados de gestión de identidades y administración de sistemas operativos, firmware y bases de datos; aplicar la suspensión ante vacaciones, incapacidades, permisos, licencias o situaciones administrativas y restablecerla únicamente previa autorización cuando corresponda. Evidencia: solicitudes de suspensión/reactivación, registros de directorio, bitácoras de sistemas y autorizaciones correspondientes.
- Configurar las carpetas de uso interno mediante permisos basados en roles y principio de mínimo privilegio, asignando acceso únicamente a los grupos o funcionarios que requieran la información para sus funciones y aplicando mecanismos de respaldo, integridad y protección contra modificaciones no autorizadas; revisar los permisos periódicamente y ante cambios de responsables o estructura organizacional. Evidencia: matriz de permisos, configuración de

carpetas, registros de acceso y reportes de revisión.

- Reportar los eventos o incidentes asociados con fallas en el aprovisionamiento de usuarios privilegiados mediante los canales establecidos para la gestión de incidentes, incluyendo como mínimo el usuario involucrado, recurso afectado, fecha y hora, descripción del evento y evidencias disponibles; efectuar el reporte inmediatamente después de identificar la pérdida, daño, robo o compromiso de activos de información. Evidencia: ticket o registro del incidente, evidencias técnicas, bitácoras y reporte de tratamiento.
- Controlar los accesos privilegiados de servidores, sistemas operativos, bases de datos y Directorio Activo mediante un inventario centralizado que relacione cada cuenta administrativa con su titular, sistema, nivel de privilegio y autorización; actualizarlo ante cada modificación y realizar como mínimo una revisión semestral para identificar cuentas huérfanas, innecesarias o excesivamente privilegiadas. Evidencia: inventario de cuentas privilegiadas, actas de revisión, reportes de directorio y registros de depuración.
- Aprovisionar los accesos a sistemas operativos y bases de datos mediante cuentas individuales, perfiles basados en roles, mínimo privilegio y mecanismos de autenticación administrados centralmente, restringiendo el uso de utilitarios que permitan modificar configuraciones o evadir controles de seguridad; validar la necesidad y autorización antes de cada asignación o modificación. Evidencia: solicitudes aprobadas, matriz de roles, configuraciones de acceso, registros de autenticación y bitácoras de actividad.
- Restringir los puertos y protocolos utilizados para mantenimiento y soporte remoto mediante reglas de firewall, listas de control de acceso y segmentación de red, habilitando únicamente los servicios, direcciones

de origen y cuentas de administradores de red autorizados; revisar las reglas periódicamente y deshabilitar las excepciones que ya no sean necesarias. Evidencia: reglas de firewall/ACL, matriz de puertos autorizados, registros de conexión y reportes de revisión.

- Gestionar los incidentes derivados del aprovisionamiento indebido de privilegios mediante el procedimiento institucional de gestión de incidentes, realizando contención, análisis de registros, identificación del alcance, corrección de permisos y seguimiento hasta el cierre; aplicar este tratamiento cada vez que se detecte pérdida, daño, robo o compromiso de activos asociado con cuentas privilegiadas. Evidencia: ticket de incidente, análisis técnico, logs, acciones de contención y reporte de cierre.

8.5.6. Restricción de acceso a la información

Control Asociado en el MSPI A.8.3

Restringir el acceso a la información, sistemas de información y aplicaciones únicamente a personal autorizado, de acuerdo con la política de control de acceso establecida en este manual. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Asignar los privilegios de acceso mediante roles y perfiles de usuario, utilizando una matriz de roles que relacione funciones, sistemas, recursos y permisos autorizados, aplicando el principio de mínimo privilegio y separación de funciones; revisar los privilegios durante la creación, modificación o retiro de cuentas y, como mínimo, periódicamente. Evidencia: matriz de roles y permisos, solicitudes aprobadas, configuraciones de acceso y registros de revisión.
- Validar la aplicación de los lineamientos de seguridad para el acceso a información electrónica mediante la revisión de los controles

configurados de acuerdo con la clasificación de la información y las condiciones autorizadas para su intercambio, verificando autenticación, autorización, cifrado y restricciones de transferencia cuando corresponda; realizar la validación durante la implementación de los controles y revisarla periódicamente o ante cambios en la clasificación o mecanismos de intercambio. Evidencia: matriz de clasificación, configuraciones de seguridad, procedimientos de intercambio, registros de validación y reportes de revisión.

- Bloquear el acceso a información sensible desde identidades no identificadas o no autorizadas, mediante mecanismos de autenticación individual, control de sesiones y listas de acceso que permitan asociar cada operación con una identidad previamente validada; aplicar el control de forma permanente y generar alertas ante intentos de acceso no autorizado. Evidencia: registros de autenticación, logs de acceso, alertas de seguridad y reportes de eventos.
- Controlar el acceso a la información mediante mecanismos de autenticación y autorización, utilizando directorio institucional, gestión de identidades, perfiles de acceso, listas de control, grupos de seguridad y, cuando aplique, autenticación multifactor; aplicar estos controles antes de conceder acceso y mantenerlos activos durante todo el ciclo de vida de la cuenta. Evidencia: configuraciones de IAM/directorio, matrices de permisos, registros de autenticación y tickets de aprovisionamiento.
- Restringir el acceso de cada usuario únicamente a los datos requeridos para sus funciones, mediante permisos asociados a roles, grupos y niveles de clasificación de la información, evitando accesos directos no justificados y aplicando el principio de mínimo privilegio; revisar los permisos ante cambios de funciones y periódicamente. Evidencia: matriz de acceso a datos, configuraciones de permisos, reportes de revisión y

solicitudes de modificación.

- Controlar las identidades y grupos autorizados para acceder a los sistemas de información mediante directorios institucionales, grupos de seguridad y mecanismos centralizados de gestión de identidades, asignando los permisos únicamente previa aprobación del responsable correspondiente; actualizar los grupos ante altas, modificaciones, traslados o retiros de usuarios. Evidencia: registros del directorio, grupos de seguridad, solicitudes aprobadas, bitácoras de cambios y reportes de depuración.
- Aplicar controles de acceso lógico a los sistemas de información mediante autenticación, autorización, perfiles de usuario, mínimo privilegio, segregación de funciones, bloqueo de cuentas y registro de actividades; verificar su funcionamiento durante la implementación, ante cambios significativos y mediante revisiones periódicas. Evidencia: políticas de acceso, configuraciones de sistemas, registros de autenticación, logs y resultados de pruebas o revisiones.
- Identificar los sistemas de información sensibles a partir de la clasificación de la información que procesan, almacenan o transmiten, utilizando el inventario de activos y la matriz de clasificación para determinar los sistemas que requieren controles reforzados; establecer y mantener ambientes tecnológicos lógicamente aislados e independientes para dichos sistemas de acuerdo con su criticidad y riesgo. Evidencia: inventario de activos, matriz de clasificación, análisis de riesgos, diagramas de arquitectura y configuraciones de segmentación.
- Aislar los sistemas que procesan información sensible mediante segmentación lógica y controles de comunicación, utilizando VLAN, firewalls, ACL, reglas de seguridad, segmentación de redes o

mecanismos equivalentes para limitar las conexiones únicamente a fuentes y destinos autorizados; revisar las reglas periódicamente y ante cambios en la arquitectura, sistemas o niveles de riesgo. Evidencia: diagramas de red, reglas de firewall/ACL, configuraciones de segmentación, registros de tráfico y reportes de revisión.

Gestión Administrativa

- Restringir el acceso a información física de acuerdo con su nivel de clasificación, mediante controles de ingreso a instalaciones, áreas restringidas, archivadores, depósitos y espacios destinados al almacenamiento de información, autorizando el acceso únicamente a las personas que tengan una necesidad funcional; revisar los permisos ante cambios de funciones, retiro de personal o modificación de las condiciones de seguridad. Evidencia: registros de acceso físico, listados de personas autorizadas, controles de ingreso, actas de revisión y registros de entrega/devolución.
- Controlar el intercambio de información física clasificada mediante mecanismos de identificación del destinatario, embalaje o protección según el nivel de clasificación, registro de entrega y confirmación de recepción; aplicar estas medidas cada vez que se transporte, entregue o transfiera documentación física clasificada. Evidencia: formatos de entrega y recepción, registros de correspondencia, actas y trazabilidad del traslado.

8.5.7. Acceso a código fuente

Control Asociado en el MSPI A.8.4

Restringir el acceso al código fuente de los sistemas de información, aplicaciones y software de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Gestionar el acceso al código fuente mediante un repositorio institucional controlado, utilizando cuentas individuales, autenticación robusta, roles y permisos diferenciados, previa autorización del responsable del sistema o proyecto; registrar y revisar periódicamente los accesos, modificaciones, descargas y demás operaciones realizadas sobre el código, conservando las trazas de auditoría de acuerdo con los tiempos de retención establecidos. Evidencia: matriz de permisos, autorizaciones, registros de autenticación, logs del repositorio y reportes de revisión.
- Proteger el código fuente almacenado en los repositorios mediante mecanismos criptográficos y de autenticación, utilizando contraseñas robustas, almacenamiento seguro de credenciales, cifrado de las comunicaciones y, cuando aplique, cifrado de la información almacenada; verificar periódicamente la configuración de estos mecanismos y corregir las desviaciones identificadas. Evidencia: configuración del repositorio, políticas de autenticación y cifrado, resultados de revisión y registros de acceso.
- Controlar el acceso a diseños, especificaciones, planes de verificación, validación y demás componentes asociados al desarrollo, mediante permisos basados en roles y asignación individual de accesos según la función desempeñada, manteniendo registro de las actividades realizadas sobre estos elementos; revisar los permisos durante cada cambio de rol, retiro del proyecto o modificación del equipo de desarrollo. Evidencia: matriz de accesos, autorizaciones, registros de actividad y reportes de revisión.
- Ejecutar las pruebas específicas sobre código fuente en un ambiente

tecnológico aislado de la red institucional y de Internet, utilizando un equipo o entorno dedicado, sin conectividad externa y con controles que impidan la transferencia no autorizada de información; aplicar esta condición antes de trasladar el código validado al ambiente de producción. Evidencia: configuración de red del ambiente de pruebas, diagramas de arquitectura, registros de pruebas y acta o autorización de paso a producción.

- Deshabilitar los puertos y mecanismos de comunicación inalámbrica de los equipos destinados a pruebas, mediante políticas de configuración de dispositivos que bloqueen USB, Bluetooth y comunicaciones por radiofrecuencia; mantener estas restricciones durante todo el período de pruebas y habilitarlas únicamente cuando exista autorización formal del responsable de Seguridad de la Información y una justificación documentada. Evidencia: políticas de configuración, registros de administración de dispositivos, autorización de excepciones y evidencias de habilitación/deshabilitación.
- Controlar el acceso de los desarrolladores al repositorio de código fuente mediante herramientas de gestión de versiones y repositorios autorizados, evitando el acceso directo a los servidores o bases de datos que soportan el repositorio y utilizando cuentas individuales para identificar cada operación; revisar los permisos y registros de actividad periódicamente y ante cambios en el equipo de desarrollo. Evidencia: configuración del repositorio, matriz de permisos, logs de actividad, registros de comités y reportes de revisión.
- Reportar los eventos o incidentes relacionados con accesos no autorizados al código fuente mediante los canales establecidos para la gestión de incidentes, proporcionando la identidad involucrada, sistema afectado, fecha y hora, actividad observada y evidencias disponibles;

realizar el reporte inmediatamente después de identificar el evento y conservar las evidencias para su análisis. Evidencia: ticket de incidente, logs, alertas de seguridad, evidencias técnicas y reporte de tratamiento.

- Validar el código fuente antes de su liberación a producción mediante controles de seguridad durante el ciclo de desarrollo, utilizando análisis estático y/o dinámico de código, revisión de dependencias, identificación de vulnerabilidades y corrección de hallazgos conforme a los criterios de seguridad establecidos; impedir el paso a producción cuando existan vulnerabilidades que superen los umbrales de aceptación definidos. Evidencia: resultados de análisis de seguridad, reporte de vulnerabilidades, registro de correcciones, aprobación de seguridad y evidencia de liberación.
- Controlar las modificaciones del código fuente y sus componentes asociados mediante el procedimiento institucional de gestión de cambios, exigiendo solicitud, justificación, análisis de impacto, revisión, aprobación, pruebas y autorización previa a la implementación; aplicar el procedimiento a toda modificación realizada sobre código, componentes, configuraciones o dependencias que pueda afectar la seguridad o funcionamiento del sistema. Evidencia: solicitud de cambio, análisis de impacto, aprobaciones, resultados de pruebas, registro de implementación y plan de reversión cuando aplique.
- Restringir la actualización y liberación del código fuente mediante controles de versiones y segregación de funciones, asegurando que la modificación, revisión, aprobación y despliegue sean trazables y, cuando la criticidad lo requiera, realizados por personas diferentes; verificar esta segregación antes de cada liberación a producción. Evidencia: historial de versiones, registros de aprobación, bitácoras de despliegue y evidencias de segregación de funciones.

- Reportar y gestionar los accesos indebidos al código fuente mediante el procedimiento de gestión de incidentes de seguridad, realizando la identificación del alcance, preservación de evidencias, contención de la cuenta o acceso comprometido, análisis de registros y aplicación de medidas correctivas; ejecutar estas acciones cada vez que se detecte un acceso no autorizado o comportamiento anómalo sobre el repositorio. Evidencia: registro del incidente, logs del repositorio, análisis técnico, acciones de contención y reporte de cierre.

8.5.8. Autenticación segura

Control Asociado en el MSPI A.8.5

Garantizar que un usuario o una entidad se autentiquen de forma segura, cuando se conceda acceso a sistemas, aplicaciones y servicios. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

Controles de autenticación y acceso

- Restringir la visualización de información del sistema antes de completar exitosamente la autenticación, mediante mecanismos de control de acceso que impidan consultar información de bases de datos, sistemas operativos, configuraciones de autenticación, Directorio Activo y demás recursos protegidos hasta validar las credenciales del usuario; aplicar el control en cada intento de inicio de sesión. Evidencia: configuración de autenticación, perfiles de acceso, registros de pruebas y logs de inicio de sesión.
- Ocultar información técnica durante el proceso de autenticación, configurando las interfaces de inicio de sesión para no revelar información que facilite la identificación de usuarios, sistemas, bases de

datos, configuraciones o mecanismos internos y deshabilitando mensajes de ayuda innecesarios; verificar esta configuración durante la implementación y después de cambios en los mecanismos de autenticación. Evidencia: configuración de los sistemas, resultados de pruebas de autenticación y registros de revisión.

- Validar las credenciales únicamente después de recibir todos los datos requeridos, mediante mecanismos de autenticación que procesen de manera controlada la totalidad de los datos de entrada antes de determinar si el acceso es válido, evitando revelar qué elemento de la credencial fue incorrecto; aplicar el control en cada intento de autenticación. Evidencia: configuración del mecanismo de autenticación, resultados de pruebas y registros de acceso.
- Limitar los intentos fallidos de autenticación mediante mecanismos de bloqueo o retraso progresivo, estableciendo un número máximo de intentos permitidos y un período de bloqueo o espera acorde con la criticidad del sistema; aplicar el control ante intentos consecutivos no exitosos y revisar periódicamente los registros para identificar patrones anómalos. Evidencia: políticas de bloqueo, configuración de umbrales, logs de autenticación y reportes de intentos fallidos.
- Registrar y monitorear los intentos fallidos de autenticación, mediante los mecanismos de auditoría de los sistemas, bases de datos, sistemas operativos y Directorio Activo, conservando como mínimo la identidad utilizada, fecha, hora, origen y resultado de la autenticación; revisar los eventos de acuerdo con la criticidad del sistema y generar alertas cuando se superen los umbrales establecidos. Evidencia: logs, alertas, reportes del SIEM o herramienta de monitoreo y registros de análisis.
- Ocultar las contraseñas durante su digitación, configurando los formularios y mecanismos de autenticación para mostrar caracteres

enmascarados y evitar su exposición visual o almacenamiento en texto claro; verificar esta condición durante las pruebas de seguridad y cada vez que se modifique la interfaz o mecanismo de autenticación. Evidencia: configuración de los sistemas, resultados de pruebas y evidencias de validación.

- Proteger los mecanismos de autenticación contra ataques de fuerza bruta, mediante bloqueo temporal de cuentas, limitación de intentos, retrasos progresivos, CAPTCHA u otros controles equivalentes, complementados con monitoreo de patrones anómalos cuando técnicamente sea aplicable; mantener estos controles activos y ajustarlos de acuerdo con los resultados de monitoreo y análisis de riesgo. Evidencia: configuración de controles, reglas de seguridad, registros de bloqueo, alertas y reportes de monitoreo.
- Generar eventos de seguridad ante intentos potenciales o violaciones exitosas de los controles de autenticación, configurando los sistemas para registrar y alertar accesos sospechosos, superación de umbrales de intentos, bloqueos, accesos exitosos posteriores a múltiples fallos y demás eventos definidos como relevantes; monitorear estos eventos de acuerdo con la criticidad del activo y gestionarlos conforme al procedimiento de incidentes cuando corresponda. Evidencia: logs, alertas, tickets de incidentes, reportes de monitoreo y análisis de eventos.
- Finalizar automáticamente las sesiones inactivas, configurando tiempos máximos de inactividad de acuerdo con la criticidad del sistema, sensibilidad de la información y nivel de privilegio del usuario; aplicar el cierre automático una vez superado el período definido y solicitar nuevamente autenticación para continuar la sesión. Evidencia: configuración de timeout, políticas de sesión, registros de cierre y

resultados de pruebas.

- Controlar la duración máxima de las conexiones, mediante parámetros de tiempo de sesión, expiración de credenciales de sesión, controles de VPN y mecanismos equivalentes, estableciendo períodos diferenciados cuando la criticidad o el nivel de privilegio lo requieran; aplicar el límite durante cada conexión y revisarlo ante cambios de riesgo o configuración. Evidencia: configuración de sesiones/VPN, políticas de acceso, logs de conexión y reportes de revisión.

Gestión de eventos e incidentes de autenticación

- Reportar los eventos e incidentes relacionados con fallas o compromisos del proceso de autenticación, mediante los canales institucionales de gestión de incidentes, incluyendo la cuenta involucrada, sistema afectado, fecha y hora, origen del evento, actividad observada y evidencias disponibles; realizar el reporte inmediatamente después de identificar una pérdida, daño, robo o compromiso de activos de información y preservar los registros para su análisis. Evidencia: ticket de incidente, logs de autenticación, alertas, análisis técnico y reporte de cierre.

Controles específicos para sistemas críticos

- Aplicar los controles de autenticación de manera diferenciada en bases de datos, sistemas operativos y Directorio Activo, configurando políticas de acceso, bloqueo de cuentas, registro de eventos, protección contra fuerza bruta, expiración de sesiones y restricciones de conexión de acuerdo con la criticidad y nivel de privilegio; verificar su configuración durante la implementación y realizar revisiones periódicas. Evidencia:

políticas de seguridad, configuraciones de sistemas, registros de auditoría y resultados de revisiones

8.6. Componente Política de Proveedores

8.6.1. Seguridad de la información en relaciones con proveedores Control Asociado en el MSPI A.5.19

Facilitar y controlar las relaciones de la ANCP-CCE con los proveedores, con el fin de verificar y gestionar adecuadamente la información a la que tienen acceso para prestar los servicios y, asegurar el cumplimiento de las políticas y procedimientos de la seguridad y privacidad de la información emitidos por la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Gestionar los requisitos de seguridad y privacidad aplicables a los proveedores mediante la identificación, clasificación y documentación de los activos, datos, sistemas, servicios y procesos a los que tendrá acceso cada proveedor, incorporando las obligaciones de confidencialidad, integridad, disponibilidad, privacidad, uso autorizado y protección de la información en los contratos, acuerdos o convenios antes del inicio del servicio. Evidencia: matriz de requisitos, evaluación de riesgos, cláusulas contractuales, acuerdos de confidencialidad y actas de aprobación.
- Realizar seguimiento al cumplimiento de los requisitos de ciberseguridad de los proveedores, mediante las actividades, controles, evaluaciones y evidencias previstas en el Lineamiento de Cumplimiento de Ciberseguridad de Proveedores y Contratistas, aplicándolos durante la selección, vinculación, ejecución, renovación y terminación de la relación contractual, con una frecuencia proporcional al nivel de riesgo del proveedor. Evidencia: evaluaciones de seguridad, informes de seguimiento, planes de tratamiento, evidencias suministradas por el

proveedor y reportes de supervisión.

- Controlar el acceso de los proveedores a los activos de información físicos, electrónicos y sistemas de información mediante autorizaciones individualizadas, perfiles basados en roles, mínimo privilegio, vigencia definida y mecanismos de autenticación y trazabilidad; revisar, modificar o revocar los permisos cuando cambie la necesidad de acceso, el alcance contractual o finalice la relación. Evidencia: matriz de accesos, solicitudes y aprobaciones, registros de autenticación, logs y actas de revocación.
- Aplicar controles de acceso durante todo el ciclo de vida de la información entregada al proveedor, desde su recolección, almacenamiento, procesamiento y transmisión hasta su devolución, eliminación o disposición final, utilizando controles técnicos, administrativos y físicos acordes con la clasificación y sensibilidad de la información. Evidencia: matriz de ciclo de vida, controles de acceso, registros de transferencia, actas de devolución/eliminación y certificados de borrado cuando corresponda.

La SIDT

- Gestionar las conexiones de equipos y dispositivos de proveedores a la infraestructura tecnológica mediante redes segmentadas, VPN, listas de control de acceso, autenticación individual y restricciones de origen/destino, estableciendo en los acuerdos de nivel de servicio las condiciones técnicas, horarios, responsables y duración de las conexiones; revisar estas condiciones ante cambios de alcance o riesgo y durante el seguimiento contractual. Evidencia: configuraciones de red, reglas de firewall/VPN, matriz de accesos, SLA y registros de conexión.
- Proteger la transmisión e intercambio de información con proveedores

mediante canales de comunicación seguros, protocolos cifrados y mecanismos de autenticación, definiendo los requisitos técnicos de acuerdo con la clasificación de la información y el nivel de riesgo del servicio; validar su configuración antes de habilitar el intercambio y revisarla ante cambios tecnológicos o contractuales. Evidencia: arquitectura de comunicaciones, configuraciones de cifrado, certificados, reglas de seguridad, pruebas de conexión y registros de transferencia.

- Proteger la información almacenada o procesada en dispositivos propiedad del proveedor mediante requisitos mínimos de configuración segura, cifrado de dispositivos y comunicaciones, control de acceso, protección contra malware, gestión de vulnerabilidades, respaldo y recuperación; verificar el cumplimiento antes de permitir el acceso a información institucional y durante la ejecución del contrato según el nivel de riesgo. Evidencia: checklist de seguridad, certificaciones, configuraciones, resultados de evaluación y evidencias entregadas por el proveedor.
- Controlar la seguridad de la información gestionada en servicios de nube contratados a proveedores mediante cláusulas que definan ubicación y residencia de los datos, responsabilidades de seguridad, gestión de accesos, cifrado, respaldo, recuperación, subcontratación, gestión de incidentes, eliminación y devolución de información; validar estos requisitos antes de contratar el servicio y durante su ejecución. Evidencia: contrato, anexos técnicos, SLA, evaluación de proveedor, certificaciones y reportes de cumplimiento.

Compras y Contratos

- Incorporar requisitos de confidencialidad y uso autorizado de la información en los contratos mediante acuerdos de confidencialidad,

cláusulas de protección de información y compromisos de uso de servicios tecnológicos, especificando las obligaciones relacionadas con datos personales, información sensible, propiedad intelectual, restricciones de divulgación y consecuencias por incumplimiento; formalizar estos compromisos antes de que el proveedor acceda a la información. Evidencia: contrato firmado, acuerdo de confidencialidad, anexos de seguridad y constancia de aceptación.

- Verificar que los colaboradores del proveedor con acceso a información institucional hayan suscrito compromisos de confidencialidad mediante la solicitud al proveedor de los soportes correspondientes y la validación de su cobertura frente al personal autorizado; realizar la verificación antes de otorgar acceso y ante la incorporación de nuevos colaboradores. Evidencia: certificación del proveedor, acuerdos de confidencialidad y listado de personal autorizado.
- Mantener actualizado el inventario de proveedores con acceso a información institucional mediante un registro centralizado que incluya proveedor, contrato, servicio, información a la que accede, nivel de clasificación, responsable, vigencia y nivel de riesgo; actualizarlo durante el alta, modificación, renovación y terminación del contrato y revisarlo periódicamente. Evidencia: registro de proveedores, matriz de acceso y reportes de actualización.
- Evaluar los riesgos de seguridad y privacidad antes de formalizar contratos que involucren información institucional, mediante la identificación de activos, amenazas, vulnerabilidades, impacto, nivel de riesgo y controles requeridos, incorporando los resultados en los requisitos y obligaciones contractuales; actualizar la evaluación cuando cambie sustancialmente el alcance o riesgo del servicio. Evidencia: evaluación de riesgos, matriz de controles y requisitos contractuales.

- Incorporar obligaciones de protección de datos personales en los contratos mediante cláusulas que establezcan las responsabilidades del proveedor respecto de recolección, acceso, tratamiento, almacenamiento, transmisión, conservación, seguridad, atención de incidentes y eliminación de datos personales; verificar su cumplimiento durante la ejecución contractual. Evidencia: contrato, anexos de tratamiento de datos, evaluaciones y reportes de supervisión.
- Incorporar criterios de seguridad de la información en el manual o instrumentos de supervisión contractual, mediante listas de verificación que permitan comprobar requisitos de acceso, confidencialidad, protección de datos, incidentes, continuidad, devolución y eliminación de información; aplicar estos criterios durante las actividades de supervisión. Evidencia: manual actualizado, checklist de supervisión y reportes de seguimiento.
- Incorporar obligaciones de recuperación, contingencia y disposición final de la información en los contratos, diferenciándolas según la clasificación, criticidad y sensibilidad de la información y estableciendo condiciones para devolución, eliminación y borrado seguro al finalizar el servicio; verificar su cumplimiento antes del cierre contractual. Evidencia: cláusulas contractuales, pruebas de recuperación, actas de devolución y certificados de eliminación segura.
- Gestión Administrativa
- Incorporar actividades de concientización en seguridad de la información para el personal de vigilancia dentro de los contratos de seguridad física, mediante contenidos sobre control de acceso, manejo de visitantes, protección de áreas restringidas, reporte de incidentes y tratamiento de información observada durante sus funciones; ejecutar las actividades al inicio del servicio y periódicamente de acuerdo con el plan de

capacitación. Evidencia: plan de capacitación, listas de asistencia, contenidos impartidos y evaluaciones.

SIDT – Desarrollo de software subcontratado

- Incorporar requisitos de desarrollo seguro en los contratos de desarrollo subcontratado mediante cláusulas que obliguen al proveedor a aplicar prácticas de desarrollo seguro, análisis de vulnerabilidades, gestión de dependencias, protección de código fuente, control de cambios, pruebas de seguridad, derechos de autor y propiedad intelectual; verificar el cumplimiento antes de cada liberación relevante y durante las evaluaciones contractuales. Evidencia: contrato, metodología de desarrollo, resultados de análisis de vulnerabilidades, informes de pruebas, repositorio de código y actas de aceptación.
- Verificar el cumplimiento de los lineamientos institucionales de desarrollo seguro mediante listas de chequeo, revisión de evidencias técnicas y validaciones de seguridad sobre los entregables del proveedor; realizar la verificación antes de autorizar la puesta en producción y ante cambios significativos. Evidencia: checklist, informes de revisión, resultados de pruebas y autorización de paso a producción.

Proveedores y terceros

- Proteger la información institucional durante su recepción, procesamiento, almacenamiento y transmisión mediante controles de acceso, cifrado, protección de dispositivos, respaldo, gestión de vulnerabilidades, medidas contra fuga de información y procedimientos de manejo seguro, aplicándolos durante toda la vigencia contractual y de acuerdo con la clasificación de la información. Evidencia: políticas y

procedimientos del proveedor, configuraciones de seguridad, registros de acceso, reportes de monitoreo y certificaciones.

- Utilizar la información institucional exclusivamente para las finalidades autorizadas en el contrato mediante controles de acceso, segregación de información, restricciones de copia y transferencia y autorización previa para usos adicionales; aplicar esta condición durante la ejecución contractual y conservar las evidencias de las autorizaciones excepcionales. Evidencia: matriz de accesos, registros de uso y transferencia, autorizaciones y reportes de auditoría.
- Formalizar los compromisos de confidencialidad y uso autorizado de la información mediante la suscripción de acuerdos por el proveedor y los colaboradores que tengan acceso a información institucional, antes de iniciar sus actividades y cada vez que se incorporen nuevos colaboradores. Evidencia: acuerdos firmados, certificaciones y listado de personal autorizado.
- Suministrar a la entidad la documentación de seguridad y privacidad requerida mediante los canales definidos contractualmente, entregando políticas, procedimientos, certificaciones, informes de evaluación y demás evidencias solicitadas; actualizar la documentación cuando existan cambios relevantes o durante las evaluaciones contractuales. Evidencia: repositorio documental, certificaciones, políticas, procedimientos e informes.
- Preservar la confidencialidad, integridad y disponibilidad de la información institucional mediante controles de acceso, protección contra modificación o destrucción no autorizada, mecanismos de respaldo y restricciones de divulgación, manteniendo estas medidas durante la relación contractual y después de su terminación cuando así lo establezca el contrato o la legislación aplicable. Evidencia: controles

implementados, registros de acceso, respaldos, informes de seguridad y declaraciones de cumplimiento.

- Impedir el uso de información institucional para beneficio propio o de terceros no autorizados mediante controles de acceso, acuerdos de confidencialidad, restricciones de copia y transferencia y monitoreo de actividades sobre información sensible; aplicar los controles durante y después de la relación contractual conforme a las obligaciones de confidencialidad. Evidencia: acuerdos, registros de acceso y transferencia, reportes de monitoreo y declaraciones de cumplimiento.
- Devolver o eliminar la información institucional al finalizar la relación contractual mediante un procedimiento documentado de devolución, destrucción o borrado seguro de archivos, bases de datos, soportes físicos y electrónicos, verificando previamente las obligaciones legales o contractuales de conservación; ejecutar la actividad durante el cierre contractual. videncia: acta de devolución, certificado de eliminación/borrado seguro, inventario de información y acta de cierre.
- Controlar la copia, reproducción, distribución o transmisión de información confidencial mediante permisos de acceso, restricciones técnicas y autorización escrita previa para cualquier transferencia no contemplada en el contrato; aplicar el control durante toda la prestación del servicio. Evidencia: autorizaciones, registros de transferencia, logs y reportes de control.
- Tratar los datos personales conforme a la legislación y condiciones contractuales aplicables mediante controles de finalidad, minimización, acceso restringido, seguridad, conservación y eliminación, limitando el tratamiento a las instrucciones y finalidades autorizadas por la entidad; verificar el cumplimiento durante las evaluaciones de seguridad y supervisión. Evidencia: acuerdo de tratamiento, registros de

tratamiento, controles de acceso, evaluaciones y reportes.

- Proteger las credenciales de acceso asignadas por la entidad mediante el uso exclusivo de cuentas individuales, autenticación segura, prohibición de compartir contraseñas y reporte inmediato de pérdida o compromiso de credenciales; aplicar estas medidas durante toda la vigencia del acceso. Evidencia: registros de autenticación, políticas de acceso, logs y reportes de incidentes.
- Capacitar al personal del proveedor que tenga acceso a información sensible mediante actividades de concientización sobre confidencialidad, protección de datos, manejo seguro, prevención de fuga de información y reporte de incidentes; ejecutar la capacitación antes del acceso y periódicamente durante la relación contractual. Evidencia: plan de capacitación, contenidos, registros de asistencia y evaluaciones.

Supervisores de contratos

- Proteger la documentación e información recibida o consultada durante la ejecución contractual mediante controles de custodia, acceso restringido, almacenamiento seguro y trazabilidad de entrega y devolución, verificando periódicamente que no existan accesos, sustracciones, modificaciones o usos no autorizados. Evidencia: registros de custodia, actas de entrega, controles de acceso y reportes de supervisión.
- Verificar que los colaboradores del proveedor con acceso a información hayan suscrito acuerdos de confidencialidad mediante la revisión documental del listado de personal autorizado y los respectivos compromisos antes de permitir o mantener el acceso; repetir la validación ante cambios en el personal del proveedor. Evidencia: certificaciones, acuerdos de confidencialidad y listado actualizado de

colaboradores.

- Coordinar las actividades de seguridad con los enlaces institucionales de Seguridad de la Información mediante reuniones, canales formales de comunicación y seguimiento de compromisos, especialmente ante cambios de alcance, incidentes, hallazgos o riesgos relevantes; realizar la coordinación durante la ejecución contractual cuando la naturaleza o riesgo del servicio lo requiera. Evidencia: actas, correos, tickets, compromisos y reportes de seguimiento.
- Verificar el cumplimiento de las medidas de seguridad y privacidad aplicables al contrato mediante listas de chequeo, revisión de evidencias y seguimiento a los requisitos legales, contractuales y técnicos definidos; realizar la verificación durante la supervisión periódica y ante cambios relevantes del servicio. Evidencia: checklist, informes de supervisión, evidencias del proveedor y registros de hallazgos.
- Reportar los incidentes de seguridad o privacidad mediante los canales institucionales definidos, suministrando la información disponible sobre el evento, activo afectado, proveedor involucrado, fecha, impacto y evidencias; efectuar el reporte inmediatamente después de conocer el incidente y realizar seguimiento hasta su cierre. Evidencia: ticket de incidente, comunicaciones, informes de análisis y seguimiento.
- Gestionar los accesos de los proveedores a los activos institucionales mediante solicitudes formalizadas, autorización del responsable de la información, asignación de permisos mínimos, definición de vigencia y posterior revocación; revisar los accesos ante cambios de personal, funciones, alcance o terminación contractual. Evidencia: solicitudes, autorizaciones, matriz de accesos, registros de aprovisionamiento y revocación.
- Solicitar y verificar la suscripción de acuerdos de confidencialidad antes

de habilitar el acceso del proveedor a información institucional, mediante la recopilación y validación de los documentos firmados por el personal autorizado, con especial atención a información que contenga datos personales o información sensible. Evidencia: acuerdos firmados, certificación del proveedor y listado de personal autorizado.

- Identificar y gestionar los riesgos de seguridad y privacidad asociados al contrato mediante la evaluación de los activos, información, amenazas, vulnerabilidades, impacto y controles aplicables; actualizar la evaluación cuando cambie el alcance, tecnología, proveedor, tipo de información o nivel de exposición. Evidencia: matriz de riesgos, evaluación de seguridad, plan de tratamiento y seguimiento de controles.
- Gestionar las evaluaciones de seguridad y privacidad solicitadas por Seguridad de la Información mediante la coordinación con el proveedor, recopilación de evidencias, atención de requerimientos y seguimiento de hallazgos y planes de tratamiento; ejecutar las evaluaciones dentro de los plazos definidos según el riesgo y criticidad del contrato. Evidencia: solicitudes de evaluación, evidencias del proveedor, informes, hallazgos y planes de tratamiento.
- Documentar en los informes de supervisión el cumplimiento de los requisitos de seguridad y privacidad mediante un apartado o lista de verificación que registre controles revisados, evidencias obtenidas, incumplimientos, incidentes, riesgos, acciones correctivas y estado de los compromisos; realizar el registro en cada informe periódico de supervisión. Evidencia: informes de supervisión, checklist, actas, evidencias del proveedor y seguimiento a compromisos.

8.6.2. Acuerdos con proveedores

Control Asociado en el MSPI A.5.20

Establecer los requisitos de seguridad y privacidad de la información, pertinentes con cada proveedor que pueda procesar, almacenar, comunicar, suministrar y tener acceso a la información de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Verificar la incorporación de las políticas y procedimientos de seguridad y privacidad de la información en los procesos de contratación, mediante la revisión de los estudios previos, anexos técnicos, términos de referencia y documentos contractuales antes de su publicación o formalización; validar que los requisitos aplicables al objeto y nivel de riesgo del contrato se encuentren incluidos. Evidencia: lista de verificación, concepto o revisión de seguridad, documentos precontractuales y contrato.
- Validar las medidas de protección aplicables a los equipos utilizados por los proveedores para procesar información institucional, mediante la inclusión de requisitos mínimos de configuración segura, control de acceso, protección contra malware, gestión de vulnerabilidades, cifrado y protección de dispositivos; realizar la validación antes de autorizar el procesamiento de información institucional y durante las evaluaciones de seguridad del proveedor. Evidencia: requisitos técnicos contractuales, checklist de seguridad, configuraciones y resultados de evaluación.
- Verificar la incorporación de requisitos de continuidad e incidentes de seguridad y privacidad en los acuerdos con proveedores, mediante la definición de responsabilidades, tiempos de respuesta, mecanismos de escalamiento, canales de atención, notificación de incidentes, recuperación del servicio y participación del proveedor en las actividades

de continuidad; validar estos requisitos antes de la formalización del contrato y durante su seguimiento. Evidencia: cláusulas contractuales, SLA, procedimiento de incidentes, plan de continuidad y registros de pruebas o ejercicios cuando apliquen.

- Validar la incorporación de mecanismos de cifrado y controles técnicos para el intercambio de información con proveedores, mediante la especificación de protocolos seguros, cifrado en tránsito y, cuando corresponda, en reposo, autenticación de los extremos y restricciones sobre medios de transferencia; verificar su configuración antes de habilitar el intercambio y ante cambios en el servicio. Evidencia: anexos técnicos, configuraciones de cifrado, certificados, pruebas de comunicación y registros de transferencia.

Compras y Contratos

- Incorporar en los contratos las medidas de seguridad y privacidad requeridas para proteger la información institucional, mediante cláusulas y anexos técnicos que especifiquen controles de acceso, confidencialidad, protección de datos personales, cifrado, gestión de incidentes, continuidad, respaldo, recuperación, devolución y eliminación de información, de acuerdo con la clasificación y riesgo del servicio; validar estos requisitos antes de la suscripción del contrato. Evidencia: contrato, anexos de seguridad, matriz de requisitos y lista de verificación.
- Incorporar en el Manual de Contratación los criterios para gestionar la seguridad y privacidad de la información en las relaciones con proveedores, mediante la definición de requisitos mínimos, responsabilidades, puntos de control y evidencias que deben verificarse durante las etapas precontractual, contractual y de cierre; revisar y

actualizar estos criterios cuando se modifique el marco normativo o institucional aplicable. Evidencia: Manual de Contratación actualizado, control de cambios y registros de aprobación.

Supervisores de contratos

- Verificar los requisitos legales y regulatorios aplicables al contrato mediante una lista de chequeo que contemple protección de datos personales, propiedad intelectual, derechos de autor, confidencialidad y demás obligaciones relacionadas con el objeto contractual; realizar la validación antes de iniciar el servicio y cuando se produzcan cambios normativos o contractuales relevantes. Evidencia: lista de verificación, concepto jurídico, contrato y anexos aplicables.
- Verificar que los acuerdos establezcan las medidas de respaldo y recuperación de la información gestionada por los proveedores, mediante la definición de alcance, frecuencia, retención, RPO, RTO, ubicación o segregación de las copias, mecanismos de protección y procedimientos de restauración; validar estos requisitos antes del inicio del servicio y verificar su cumplimiento durante la supervisión contractual. Evidencia: cláusulas contractuales, SLA, políticas de respaldo, reportes de ejecución y resultados de pruebas de restauración.
- Controlar el acceso de los proveedores a los activos institucionales mediante solicitudes formalizadas, autorización previa, identificación individual, perfiles basados en roles, mínimo privilegio, vigencia definida y revocación al finalizar la necesidad de acceso; revisar los permisos ante cambios de personal, funciones, alcance contractual o terminación del contrato. Evidencia: solicitudes y autorizaciones, matriz de accesos, registros de aprovisionamiento/revocación y logs.
- Validar los requisitos de seguridad aplicables a los dispositivos propiedad

del proveedor que almacenen o procesen información institucional, mediante una lista de controles que contemple configuración segura, actualización, protección contra malware, cifrado, control de acceso, respaldo y gestión de vulnerabilidades; realizar la validación antes de autorizar el acceso y periódicamente según el nivel de riesgo. Evidencia: checklist, resultados de evaluación, certificaciones del proveedor y registros de cumplimiento.

- Verificar la formalización de los acuerdos de confidencialidad y no divulgación, mediante la recopilación y revisión de los documentos firmados por el proveedor y por los colaboradores que tengan acceso a información institucional; efectuar la verificación antes de habilitar el acceso y ante la incorporación de nuevos colaboradores. Evidencia: acuerdos firmados, certificación del proveedor y listado actualizado de personal autorizado.

Proveedores y terceros

- Proteger la información pública clasificada y pública reservada suministrada por la ANCP-CCE mediante controles de acceso restringido, autenticación individual, almacenamiento seguro, cifrado cuando corresponda, protección contra pérdida o modificación y mecanismos de respaldo, aplicándolos durante todo el período en que la información se encuentre bajo su custodia o tratamiento. Evidencia: políticas y procedimientos del proveedor, matriz de accesos, registros de actividad, configuraciones de seguridad y reportes de cumplimiento.
- Tratar los datos personales únicamente para las finalidades autorizadas en el contrato, mediante controles de acceso, minimización, confidencialidad, protección de los datos, conservación limitada y eliminación o devolución al finalizar la finalidad o relación contractual,

de acuerdo con las instrucciones de la entidad y la normativa aplicable. Evidencia: acuerdo de tratamiento de datos, registros de tratamiento, controles de acceso, evidencias de eliminación/devolución y reportes de cumplimiento.

- Aplicar las obligaciones de seguridad y privacidad establecidas contractualmente y en el Manual Operativo del SGSI, mediante procedimientos internos, controles técnicos, administrativos y físicos, capacitación del personal y mecanismos de seguimiento; mantener su cumplimiento durante toda la vigencia del contrato y atender las acciones correctivas derivadas de las verificaciones realizadas por la entidad. Evidencia: procedimientos, registros de capacitación, evidencias de controles, evaluaciones y planes de acción.
- Reportar los incidentes de seguridad y privacidad de la información mediante los canales institucionales definidos en el contrato y los procedimientos de gestión de incidentes, proporcionando como mínimo la fecha y hora de detección, activo afectado, descripción del evento, impacto conocido y evidencias disponibles; realizar la notificación dentro de los tiempos establecidos contractualmente y mantener comunicación hasta su cierre. Evidencia: ticket o comunicación del incidente, registros de escalamiento, evidencias técnicas, informes de análisis y reporte de cierre.
-

8.6.3. Gestión de seguridad de la cadena de suministro TIC

Control Asociado en el MSPI A.5.21

Definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC en la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Compras y Contratos

- Incorporar los requisitos de seguridad y privacidad de la información en los contratos de adquisición de productos y servicios de tecnologías de la información y las comunicaciones, mediante cláusulas, anexos técnicos y condiciones contractuales que contemplen controles de acceso, confidencialidad, protección de datos, gestión de vulnerabilidades, incidentes, continuidad, respaldo, recuperación y eliminación segura, de acuerdo con la clasificación de la información y el nivel de riesgo. Aplicar antes de la formalización del contrato y actualizar ante modificaciones del objeto, alcance, servicio o nivel de riesgo. Evidencia: contratos, anexos técnicos, matriz de requisitos y listas de verificación contractual.
- Incorporar garantías de seguridad para la cadena de suministro de TIC mediante cláusulas que establezcan requisitos de seguridad para proveedores, subcontratistas, componentes y servicios, incluyendo gestión de vulnerabilidades, protección contra alteraciones, trazabilidad, notificación de incidentes, continuidad y cumplimiento de requisitos de seguridad. Verificar su inclusión antes de la formalización y ante modificaciones relevantes de la cadena de suministro. Evidencia: contratos, anexos de seguridad, declaraciones o certificaciones de proveedores y registros de revisión contractual.

Seguridad de la Información

- Evaluar y documentar los riesgos de seguridad de la información asociados a los requisitos y acuerdos de la cadena de suministro, mediante la aplicación de la metodología institucional de gestión de riesgos sobre proveedores, productos, servicios, componentes críticos,

subcontratistas y dependencias tecnológicas. Realizar la evaluación antes de la contratación y actualizarla ante cambios significativos, nuevos riesgos, incidentes o modificaciones en la cadena de suministro. Evidencia: matriz de riesgos, análisis de impacto, valoración de riesgos y registros de actualización.

- Verificar la incorporación de obligaciones de seguridad para la cadena de suministro mediante la revisión de estudios previos, anexos técnicos, acuerdos de nivel de servicio y contratos, comprobando que incluyan requisitos de protección de información, gestión de incidentes, continuidad, confidencialidad, vulnerabilidades, subcontratación y cumplimiento normativo. Realizar la verificación antes de la formalización contractual y durante las modificaciones contractuales. Evidencia: listas de verificación, conceptos de revisión, contratos y anexos aprobados.

La SIDT

- Incorporar prácticas de seguridad de la cadena de suministro en los contratos con proveedores de productos TIC mediante requisitos de seguridad aplicables a fabricantes, distribuidores, integradores y subcontratistas, incluyendo protección de componentes, gestión de vulnerabilidades, actualizaciones, trazabilidad y notificación de incidentes. Exigir su cumplimiento antes de la entrega o puesta en operación y verificarlo durante la ejecución contractual. Evidencia: cláusulas contractuales, fichas técnicas, certificaciones, informes de evaluación y actas de recibo.
- Incorporar requisitos de seguridad de la información y gestión de riesgos en los contratos de adquisición de productos y servicios TIC mediante anexos técnicos y condiciones de seguridad definidos según la criticidad,

clasificación de la información, arquitectura tecnológica y riesgos identificados. Aplicar antes de la contratación y revisar ante cambios tecnológicos, contractuales o de riesgo. Evidencia: anexos técnicos, matriz de requisitos, evaluación de riesgos y contrato.

- Verificar que los productos y servicios TIC sean entregados conforme a las especificaciones contractuales mediante listas de chequeo, pruebas técnicas, validación de características de seguridad, revisión de documentación y aceptación formal de los entregables. Realizar la verificación antes de la aceptación de cada entrega y durante los hitos definidos contractualmente. Evidencia: actas de recibo, resultados de pruebas, listas de chequeo, informes técnicos y registros de aceptación.
- Exigir la comunicación de los requisitos de seguridad y privacidad a los integrantes de la cadena de suministro mediante cláusulas contractuales que obliguen a proveedores y subcontratistas a transmitir dichas condiciones a las partes que intervengan en la prestación del servicio o suministro. Aplicar desde el inicio de la relación contractual y ante la incorporación de nuevos subcontratistas o terceros. Evidencia: cláusulas contractuales, certificaciones de cumplimiento, registros de comunicación y relación actualizada de subcontratistas.
- Identificar y documentar los componentes críticos de los productos y servicios TIC mediante inventarios, diagramas de arquitectura, fichas técnicas, análisis de dependencias y evaluación de criticidad, considerando aquellos cuya falla, alteración o indisponibilidad pueda afectar la confidencialidad, integridad o disponibilidad de la información. Realizar la identificación durante la adquisición y actualizarla ante cambios de arquitectura, componentes o servicios. Evidencia: inventario de componentes críticos, diagramas, fichas técnicas y análisis de criticidad.

- Verificar las condiciones de seguridad del aprovisionamiento de servicios en la nube, telecomunicaciones y hardware mediante listas de chequeo y validaciones técnicas que contemplen controles de acceso, cifrado, disponibilidad, continuidad, gestión de vulnerabilidades, ubicación de la información, respaldo, soporte y responsabilidades de seguridad. Realizar la verificación antes de la contratación o puesta en producción y periódicamente durante la prestación del servicio, de acuerdo con su criticidad y riesgo. Evidencia: evaluaciones de proveedores, listas de chequeo, certificaciones, informes técnicos, SLA y registros de seguimiento.

Supervisores de los contratos

- Notificar las situaciones que puedan generar riesgos en el suministro de productos y servicios TIC mediante los canales institucionales de gestión contractual y seguridad, registrando la descripción de la novedad, servicio o componente afectado, impacto identificado, proveedor involucrado y evidencias disponibles. Realizar la notificación inmediatamente después de identificar la situación y efectuar seguimiento hasta su tratamiento o cierre. Evidencia: tickets, comunicaciones formales, reportes de supervisión, registros de riesgos y evidencias técnicas.
- Monitorear las novedades relacionadas con el suministro de productos y servicios TIC mediante la revisión de entregables, niveles de servicio, cambios, incidentes, vulnerabilidades, incumplimientos y compromisos establecidos contractualmente. Realizar el seguimiento durante toda la ejecución contractual y con la periodicidad definida en el contrato o según la criticidad del servicio. Evidencia: informes de supervisión, actas de seguimiento, indicadores de SLA, registros de incidentes, planes de

acción y comunicaciones con proveedores.

8.6.4. Supervisión de servicios de proveedores

Control Asociado en el MSPI A.5.22

Monitorear y revisar la prestación de servicios de proveedores para asegurar que cumplan con los requisitos de seguridad. Por lo tanto, se desarrollarán las siguientes actividades:

Compras y Contratos

- Incorporar en los procedimientos de gestión contractual las actividades, criterios y puntos de control para realizar el seguimiento, revisión y gestión de cambios de los servicios suministrados por proveedores, mediante la definición de etapas de solicitud, análisis de impacto, aprobación, implementación, validación y cierre. Aplicar durante toda la ejecución contractual y ante cualquier modificación del servicio, alcance, tecnología, proveedor o condición de seguridad. Evidencia: procedimientos, formatos de solicitud de cambio, registros de aprobación, actas de seguimiento y reportes de cierre.
- Aplicar un mecanismo de gestión de deficiencias en la prestación de servicios mediante el registro del incumplimiento, análisis de impacto, definición de acciones correctivas, establecimiento de plazos y seguimiento hasta su cierre. Activar cada vez que se identifique un incumplimiento de los niveles de servicio, requisitos de seguridad, privacidad o condiciones contractuales. Evidencia: reportes de supervisión, registros de incumplimientos, planes de acción, comunicaciones al proveedor y evidencias de cierre.

La SIDT

- Gestionar los cambios de infraestructura, sistemas de información y

servicios tecnológicos soportados por proveedores mediante el procedimiento institucional de gestión de cambios, que incluya solicitud, análisis de impacto técnico y de seguridad, evaluación de riesgos, aprobación, pruebas, implementación controlada, validación y reversión cuando sea necesario. Aplicar antes de implementar cualquier cambio y realizar validaciones posteriores para confirmar su efectividad, seguridad y calidad. Evidencia: solicitudes de cambio, análisis de impacto, aprobaciones, resultados de pruebas, registros de implementación y validación posterior.

- Monitorear los permisos de acceso asignados a proveedores mediante la revisión de cuentas, roles, privilegios, fechas de vigencia y registros de autenticación en las herramientas de gestión de identidades y sistemas de información. Realizar seguimiento periódico y efectuar revisión inmediata ante cambios de personal, funciones, alcance contractual, terminación del servicio o identificación de accesos innecesarios. Evidencia: matriz de accesos, solicitudes y aprobaciones, registros de creación/modificación/revocación, reportes de revisión y logs de acceso.
- Incorporar cláusulas para la identificación y gestión de vulnerabilidades en los contratos de tecnología mediante requisitos de evaluación, reporte, clasificación, remediación y seguimiento de vulnerabilidades de productos, componentes y servicios suministrados. Aplicar cuando la naturaleza, criticidad o exposición del servicio justifique el requisito y verificar su cumplimiento durante la ejecución contractual. Evidencia: cláusulas contractuales, informes de vulnerabilidades, planes de remediación, resultados de pruebas y reportes de seguimiento.
- Incorporar en los contratos la facultad de realizar auditorías o evaluaciones de seguridad a los proveedores mediante cláusulas que establezcan alcance, condiciones de acceso, periodicidad, entrega de

evidencias y tratamiento de hallazgos. Activar el mecanismo ante cambios relevantes en los servicios, incidentes, incumplimientos, riesgos elevados o cuando sea requerido por la evaluación de seguridad. Evidencia: cláusulas contractuales, planes de auditoría, solicitudes de evidencia, informes de auditoría y planes de tratamiento.

- Incorporar la participación del responsable del plan de recuperación de desastres en la evaluación de cambios que puedan afectar la continuidad mediante su convocatoria a los análisis y comités de cambio con capacidad para emitir observaciones y participar en la decisión de aprobación. Aplicar antes de aprobar cambios que puedan modificar el RTO, RPO, disponibilidad, dependencias críticas o mecanismos de recuperación. Evidencia: convocatorias, actas, análisis de impacto, conceptos de continuidad y registros de aprobación.

- Gestionar los cambios derivados de la ejecución de contratos mediante el registro de cada solicitud, análisis de impacto, evaluación de riesgos, aprobación, implementación, pruebas y validación posterior, considerando como mínimo modificaciones en:

- sistemas de información;
- políticas de seguridad de la información;
- procedimientos operativos;
- controles de seguridad;
- actividades de mantenimiento;
- infraestructura y servicios tecnológicos.

- Aplicar antes de implementar cualquier modificación y realizar validación posterior cuando el cambio pueda afectar la seguridad, disponibilidad, integridad, confidencialidad o continuidad. Evidencia: registro de

cambios, análisis de impacto, aprobaciones, resultados de pruebas, actas de implementación y validaciones posteriores.

Supervisores de los contratos

- Revisar y actualizar la información y condiciones de seguridad de los proveedores mediante la validación de contratos vigentes, servicios suministrados, responsables, accesos, riesgos, ANS y requisitos de seguridad, con apoyo de los enlaces de seguridad de la información. Realizar como mínimo una revisión anual al inicio de cada período y adicionalmente ante cambios relevantes, incidentes, modificaciones contractuales o nuevas condiciones de riesgo. Evidencia: matriz o registro actualizado de proveedores, listas de verificación, actas de revisión, evaluaciones de riesgo y registros de actualización.
- Verificar periódicamente el cumplimiento de los Acuerdos de Nivel de Servicio, acuerdos de confidencialidad y acuerdos de intercambio de información mediante la comparación de los compromisos contractuales con los resultados efectivamente obtenidos y la revisión de indicadores, incidentes y excepciones. Realizar la verificación con la periodicidad establecida en el contrato y registrar los incumplimientos identificados. Evidencia: informes de supervisión, indicadores ANS, actas, acuerdos vigentes, registros de incumplimientos y planes de acción.
- Realizar seguimiento a la prestación de los servicios mediante la revisión de controles de seguridad y privacidad, cumplimiento de obligaciones contractuales, gestión de incidentes, tratamiento de hallazgos y ejecución de acciones correctivas. Efectuar el seguimiento periódicamente durante toda la ejecución contractual y reforzarlo ante incidentes, incumplimientos o cambios relevantes. Evidencia: informes de supervisión, listas de verificación, registros de incidentes, planes de

acción, comunicaciones y actas de seguimiento.

- Verificar el cumplimiento de los términos y condiciones de seguridad y privacidad mediante la revisión de evidencias contractuales, técnicas y operativas, contrastándolas con las obligaciones establecidas en el contrato, anexos, acuerdos y procedimientos aplicables. Realizar la verificación durante la ejecución contractual, en los hitos de supervisión y antes del cierre del servicio. Evidencia: listas de chequeo, informes de supervisión, evidencias técnicas, actas y registros de cierre.

Proveedores de la entidad

- Reportar los incidentes de seguridad o privacidad relacionados con la prestación del servicio mediante los canales institucionales definidos, proporcionando como mínimo fecha y hora de detección, activo o servicio afectado, descripción del evento, impacto conocido y evidencias disponibles. Realizar la notificación dentro de los tiempos establecidos contractualmente y mantener actualizada la información hasta el cierre del incidente. Evidencia: tickets, comunicaciones, reportes de incidente, registros de escalamiento, evidencias técnicas y análisis de cierre.
- Respaldar y proteger los activos de información utilizados durante la prestación del servicio mediante controles acordes con su clasificación, incluyendo control de acceso, protección contra pérdida o alteración, copias de respaldo, cifrado cuando corresponda y medidas de conservación y resguardo. Aplicar durante todo el período de custodia o utilización y solicitar apoyo técnico cuando se requieran mecanismos institucionales de preservación o recuperación. Evidencia: registros de respaldo, configuraciones de seguridad, controles de acceso, reportes de ejecución, pruebas de restauración y actas de entrega o custodia.

8.6.4.1. Uso de servicios en la nube

Control Asociado en el MSPI A.5.23

Establecer procesos de adquisición, uso, gestión y salida de los servicios en la nube, de acuerdo con los requisitos de seguridad y privacidad de la información definidos por la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Incorporar los requisitos de seguridad y privacidad aplicables a IaaS, PaaS y SaaS mediante una matriz de controles que contemple clasificación de la información, gestión de identidades, mínimo privilegio, cifrado, segregación de ambientes, registro y monitoreo, respaldo, continuidad, eliminación segura, protección de datos personales y gestión de incidentes. Aplicar antes de la adquisición o migración y revisar ante cambios en el servicio, tecnología o nivel de riesgo. Evidencia: matriz de requisitos, anexo técnico, listas de verificación y concepto de seguridad.
- Evaluar los proveedores de servicios en la nube mediante una matriz de selección que valore reputación, experiencia, fiabilidad, protección de datos, certificaciones aplicables, escalabilidad, alta disponibilidad, rendimiento, soporte y modelo de costos. Realizar la evaluación antes de la contratación y actualizarla ante renovaciones, cambios significativos o nuevos riesgos. Evidencia: matriz de evaluación, certificaciones, informes de debida diligencia, resultados de evaluación y concepto de selección.
- Asignar funciones y responsabilidades para el uso y administración de servicios en la nube mediante una matriz RACI que diferencie responsabilidades de seguridad, administración, operación, continuidad, gestión de accesos, incidentes y supervisión contractual. Definirlas antes

de la puesta en operación y revisarlas ante cambios organizacionales, tecnológicos o contractuales. Evidencia: matriz RACI, procedimientos, registros de asignación y actas de aprobación.

- Gestionar los incidentes y cambios de los servicios en la nube mediante procedimientos que contemplen registro, clasificación, análisis de impacto, escalamiento, autorización, implementación, recuperación y cierre. Aplicar ante cada incidente o cambio y efectuar validación posterior cuando pueda afectar la seguridad, disponibilidad o continuidad. Evidencia: tickets, registros de cambios, análisis de impacto, bitácoras, informes de incidentes y registros de cierre.

Compras y Contratos

- Incorporar requisitos para la adquisición de servicios IaaS, PaaS y SaaS mediante lineamientos, procedimientos, anexos técnicos y listas de verificación que incluyan seguridad, privacidad, continuidad, niveles de servicio, gestión de accesos, ubicación de datos, incidentes, respaldo, recuperación y salida del servicio. Aplicar durante las etapas precontractual, contractual y de cierre. Evidencia: estudios previos, anexos técnicos, listas de verificación, contratos y actas de cierre.
- Incorporar garantías contractuales de confidencialidad, integridad y disponibilidad mediante cláusulas que establezcan controles, niveles de servicio, responsabilidades, mecanismos de protección, continuidad, recuperación y compensaciones o acciones ante incumplimientos. Validar antes de la formalización contractual y durante la supervisión del servicio. Evidencia: contrato, SLA/ANS, anexos de seguridad, certificaciones y reportes de cumplimiento.

La SIDT

- Evaluar y documentar los riesgos de seguridad y privacidad asociados a los servicios en la nube mediante la metodología institucional de gestión de riesgos, considerando proveedor, modelo IaaS/PaaS/SaaS, clasificación de información, ubicación de datos, dependencias, accesos, subcontratistas y continuidad. Realizar antes de la migración o contratación y actualizar ante cambios relevantes, incidentes o nuevos riesgos. Evidencia: matriz de riesgos, análisis de impacto, plan de tratamiento y registros de actualización.
- Solicitar y verificar la conformidad de los controles de seguridad y privacidad del proveedor mediante cuestionarios, certificaciones, informes de auditoría, evidencias técnicas y evaluaciones de cumplimiento frente a los requisitos contractuales. Realizar antes de la contratación y periódicamente durante la prestación, según criticidad y riesgo. Evidencia: evaluaciones, certificaciones, informes SOC/ISO cuando apliquen, cuestionarios y registros de verificación.
- Evaluar los servicios de cómputo en nube mediante criterios técnicos relacionados con arquitectura, disponibilidad, rendimiento, escalabilidad, seguridad, integración, recuperación, interoperabilidad, portabilidad y costos. Aplicar durante la evaluación de alternativas y antes de la adquisición o migración. Evidencia: matriz técnica, pruebas de concepto, resultados de pruebas y concepto de evaluación.
- Diseñar y probar los mecanismos de continuidad y recuperación de los servicios en nube mediante procedimientos de respaldo, recuperación, redundancia, restauración y contingencia alineados con los RTO y RPO definidos. Probarlos antes de la puesta en producción y periódicamente, así como después de cambios relevantes o incidentes. Evidencia: procedimientos, resultados de pruebas, registros de restauración,

RTO/RPO obtenidos y planes de mejora.

- Monitorear y optimizar la capacidad de los servicios en nube mediante herramientas de gestión que permitan visualizar consumo de CPU, memoria, almacenamiento, red, disponibilidad y crecimiento, ajustando recursos según demanda y criticidad. Realizar seguimiento continuo y optimización periódica. Evidencia: tableros de monitoreo, reportes de capacidad, recomendaciones y registros de ajustes.
- Establecer y verificar los ANS con los proveedores mediante acuerdos que definan tiempos de atención, respuesta, recuperación, disponibilidad, escalamiento y tratamiento de fallas y requerimientos. Validar los niveles acordados durante la contratación y monitorearlos durante toda la prestación del servicio. Evidencia: ANS/SLA, reportes de disponibilidad, tickets, indicadores y actas de seguimiento.
- Incorporar cláusulas de propiedad de la información y propiedad intelectual mediante disposiciones contractuales que reconozcan la titularidad de la entidad sobre la información agregada, creada, generada, modificada o almacenada durante la prestación del servicio. Aplicar durante toda la vigencia contractual y verificar su cumplimiento al cierre del servicio. Evidencia: contrato, anexos de propiedad intelectual y actas de cierre.
- Incorporar requisitos de eliminación segura de la información mediante cláusulas que establezcan métodos de borrado seguro, eliminación de copias, medios afectados, plazos y entrega de certificación de eliminación al finalizar el contrato o cuando corresponda. Aplicar al cierre contractual, terminación anticipada o migración del servicio. Evidencia: certificación de eliminación, actas de cierre, registros técnicos y constancias del proveedor.
- Incorporar el derecho de acceso a reportes de seguridad, continuidad y

riesgos mediante cláusulas que obliguen al proveedor a suministrar las evidencias y reportes requeridos, preservando la confidencialidad de la información del proveedor cuando corresponda. Solicitar durante la ejecución contractual cuando se requiera para supervisión, auditoría, gestión de riesgos o incidentes. Evidencia: cláusulas contractuales, solicitudes, informes recibidos y registros de revisión.

- Aplicar criterios de seguridad y privacidad al aprovisionamiento de recursos mediante plantillas, configuraciones base, listas de chequeo y controles técnicos que incorporen mínimo privilegio, cifrado, segmentación, registro, monitoreo y endurecimiento. Aplicar desde la creación de cada recurso y verificar ante cambios de configuración. Evidencia: plantillas, configuraciones, registros de aprovisionamiento y resultados de validación.
- Segregar los ambientes de desarrollo, pruebas y producción mediante cuentas, suscripciones, proyectos o redes independientes y controles diferenciados de acceso y administración. Aplicar desde el diseño y mantener durante todo el ciclo de vida; verificar ante cambios de arquitectura. Evidencia: arquitectura, configuración de cuentas/suscripciones, matrices de acceso y diagramas de red.
- Aplicar controles diferenciados para desarrollo, pruebas y producción mediante configuraciones, datos, accesos, credenciales y permisos específicos para cada ambiente. Verificar antes de la puesta en producción y después de cambios relevantes. Evidencia: configuraciones, matrices de acceso, registros de despliegue y resultados de pruebas.
- Separar ambientes y servicios de seguridad mediante cuentas, suscripciones o proyectos independientes, evitando que una falla o compromiso en un ambiente afecte directamente a los demás. Aplicar

durante el diseño y revisar periódicamente o ante cambios de arquitectura. Evidencia: arquitectura cloud, configuración de cuentas y resultados de revisión.

- Segmentar las redes de nube mediante redes, subredes, grupos de seguridad y controles perimetrales diferenciados para servidores web, aplicaciones y bases de datos, restringiendo las comunicaciones a los flujos autorizados. Aplicar durante el aprovisionamiento y verificar ante cada cambio de arquitectura o reglas. Evidencia: diagramas, reglas de firewall, grupos de seguridad, ACL y pruebas de conectividad.
- Gestionar las identidades y accesos mediante IAM, roles, autenticación multifactor, mínimo privilegio, cuentas individuales y revisiones periódicas de permisos. Aplicar desde la creación de las cuentas y revisar como mínimo periódicamente y ante cambios de funciones o desvinculaciones. Evidencia: matrices de acceso, registros IAM, configuraciones MFA, logs y actas de revisión.
- Restringir el tráfico entrante y saliente mediante reglas de firewall, grupos de seguridad, ACL y listas de control basadas en origen, destino, puerto y protocolo autorizado. Aplicar durante el aprovisionamiento y revisar periódicamente y ante cambios de servicio. Evidencia: configuraciones, reglas aprobadas, logs y resultados de pruebas.
- Implementar conexiones VPN o enlaces dedicados entre los ambientes cloud y On-premise mediante canales autenticados y cifrados, restringiendo las rutas y servicios permitidos. Aplicar cuando exista intercambio de información o dependencia operativa entre ambientes y validar periódicamente su configuración. Evidencia: configuración VPN/enlace, diagramas, registros de conexión y pruebas de comunicación.
- Aplicar cifrado de información en tránsito y en reposo mediante

protocolos seguros, mecanismos criptográficos institucionales y gestión controlada de llaves, de acuerdo con la clasificación de la información. Aplicar durante el almacenamiento, transmisión y procesamiento de información confidencial y verificar ante cambios de plataforma. Evidencia: configuraciones criptográficas, certificados, políticas de llaves y resultados de pruebas.

- Gestionar el aprovisionamiento, modificación y actualización de recursos cloud mediante el proceso institucional de gestión de cambios, incluyendo análisis de impacto, autorización, pruebas y validación posterior. Aplicar antes de implementar cambios en producción. Evidencia: solicitudes de cambio, aprobaciones, resultados de pruebas y registros de implementación.
- Mantener actualizado el inventario de recursos cloud mediante herramientas de descubrimiento, registros de activos y etiquetado, incluyendo cuentas, suscripciones, máquinas virtuales, bases de datos, almacenamiento, redes y servicios administrados. Actualizar de forma automática cuando sea posible y verificar periódicamente. Evidencia: inventario, reportes de descubrimiento y registros de actualización.
- Incorporar los recursos cloud al proceso de gestión de vulnerabilidades mediante herramientas de evaluación, actualización y aplicación de parches, priorizando según criticidad, exposición y severidad. Realizar evaluaciones periódicas y aplicar correcciones conforme a los SLA de remediación definidos. Evidencia: reportes de vulnerabilidades, tickets de remediación, registros de parches y verificaciones posteriores.
- Etiquetar los recursos cloud mediante convenciones estandarizadas que permitan identificar propietario, servicio, ambiente, criticidad, centro de costo y propósito. Aplicar durante el aprovisionamiento y validar periódicamente la cobertura y consistencia de las etiquetas. Evidencia:

políticas de etiquetado, inventarios, reportes de cumplimiento y registros de costos.

Supervisores de los contratos

- Gestionar los incidentes de seguridad y privacidad asociados a servicios cloud mediante los canales definidos en el contrato y procedimiento institucional, realizando registro, escalamiento, seguimiento, análisis de impacto y cierre. Aplicar ante cada incidente y mantener seguimiento hasta la implementación de las acciones correctivas. Evidencia: tickets, comunicaciones, informes de incidentes, planes de acción y registros de cierre.
- Monitorear y evaluar continuamente el uso de los servicios cloud mediante la revisión de indicadores de seguridad, disponibilidad, consumo, accesos, incidentes, vulnerabilidades y cambios, actualizando la evaluación de riesgos cuando corresponda. Realizar seguimiento periódico según la criticidad del servicio y ante eventos relevantes. Evidencia: informes de supervisión, indicadores, evaluaciones de riesgo, reportes del proveedor y planes de acción.
- Verificar las prácticas y procedimientos de seguridad del proveedor mediante la revisión de certificaciones, políticas, auditorías, evaluaciones independientes, resultados de controles y evidencias de cumplimiento contractual. Realizar antes de la contratación y periódicamente durante la prestación del servicio. Evidencia: certificaciones, informes de auditoría, cuestionarios, evaluaciones y actas de seguimiento.
- Verificar las condiciones jurídicas aplicables al país o territorio donde se almacene o procese información, mediante la revisión de las condiciones de transferencia o transmisión internacional y de las garantías de

protección de datos personales exigibles conforme al marco jurídico colombiano. Realizar antes de la migración o contratación y ante cambios en la ubicación, proveedor o jurisdicción de tratamiento. Evidencia: evaluación jurídica, contrato, cláusulas de transferencia, ubicación declarada de datos y registros de aprobación.

- Analizar periódicamente los costos de los recursos cloud mediante reportes de consumo, facturación, tendencias, presupuestos y alertas de variación, identificando recursos sobredimensionados, no utilizados o con consumos atípicos. Realizar análisis periódico y ante incrementos significativos o desviaciones presupuestales. Evidencia: reportes de costos, tableros de consumo, análisis de variaciones, alertas y acciones de optimización.

Administradores de la nube

- Aplicar controles técnicos y operativos para preservar la confidencialidad, integridad y disponibilidad mediante gestión de accesos, cifrado, respaldo, monitoreo, redundancia, gestión de vulnerabilidades y recuperación. Mantener durante toda la operación y verificar mediante revisiones periódicas y pruebas de control. Evidencia: configuraciones, logs, reportes de monitoreo, respaldos, pruebas de recuperación y resultados de auditoría.
- Evaluar la información susceptible de migración a la nube mediante la revisión de clasificación, criticidad, requisitos legales, dependencias, ubicación, controles disponibles y riesgos asociados al servicio cloud seleccionado. Realizar antes de cada migración y reevaluar ante cambios en clasificación, proveedor o arquitectura. Evidencia: inventario de información, análisis de migración, matriz de clasificación y concepto técnico.

- Aplicar la metodología institucional de gestión de riesgos para evaluar la migración de información a la nube, considerando amenazas, vulnerabilidades, impacto sobre la confidencialidad, integridad y disponibilidad, controles existentes y riesgo residual. Realizar antes de autorizar la migración y actualizar ante cambios relevantes. Evidencia: matriz de riesgos, valoración, plan de tratamiento y aprobación de migración.
- Asignar roles y responsabilidades técnicas para el uso de la nube mediante matrices de permisos, roles administrativos, funciones operativas y reglas de segregación de funciones. Aplicar durante el aprovisionamiento de cuentas y revisar ante cambios de personal, funciones o servicios. Evidencia: matriz de roles, configuraciones IAM, solicitudes de acceso y registros de revisión.
- Reportar los eventos e incidentes de seguridad o privacidad relacionados con la nube mediante los canales institucionales definidos, incluyendo información sobre recurso afectado, fecha y hora, evento detectado, impacto, acciones ejecutadas y evidencias disponibles. Realizar la notificación inmediatamente después de su identificación y efectuar seguimiento hasta su escalamiento o cierre. Evidencia: tickets, alertas, logs, reportes técnicos, comunicaciones y registros de cierre.

8.7. Componente Política de gestión de Eventos

8.7.1. Gestión de incidentes de seguridad de la información Control Asociado en el MSPI A.5.24

Establecer capacidades para la gestión efectiva de incidentes de seguridad. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Documentar y mantener actualizados los procedimientos, lineamientos y criterios para la evaluación y gestión de incidentes de seguridad y privacidad de la información, mediante la definición del ciclo de identificación, registro, clasificación, análisis, contención, erradicación, recuperación, cierre y lecciones aprendidas, en conjunto con los procedimientos técnicos aplicables. Revisar como mínimo anualmente y actualizar ante cambios normativos, tecnológicos, organizacionales o derivados de incidentes relevantes. Evidencia: procedimientos aprobados, matrices de clasificación, formatos de gestión y registros de actualización.
- Coordinar la atención de los incidentes mediante un flujo de gestión que establezca responsables de atención, canales de comunicación, niveles de escalamiento, tiempos de respuesta y mecanismos de coordinación con proveedores y entidades externas, incluyendo, cuando corresponda, ColCERT, Comando Conjunto Cibernético, Policía Nacional de Colombia, CSIRT Gobierno y Superintendencia de Industria y Comercio. Activar el flujo según la severidad, impacto, naturaleza del incidente y obligaciones legales o contractuales aplicables. Evidencia: tickets, registros de escalamiento, comunicaciones, actas, reportes de incidente y registros de coordinación externa.
- Evaluar y clasificar los incidentes mediante criterios previamente definidos de impacto, alcance, criticidad, activos afectados, información comprometida y nivel de riesgo, asignando prioridad y tratamiento conforme a la metodología institucional. Aplicar desde la identificación del evento y actualizar la clasificación cuando se obtenga nueva información sobre su impacto o alcance. Evidencia: registro del incidente, matriz de clasificación, valoración de impacto y trazabilidad de cambios.

- Responder y gestionar los incidentes mediante actividades documentadas de contención, análisis, erradicación, recuperación y cierre, priorizando la protección de la confidencialidad, integridad y disponibilidad de los activos afectados. Aplicar de acuerdo con la criticidad del incidente y los tiempos de respuesta establecidos. Evidencia: bitácora del incidente, acciones ejecutadas, registros técnicos, resultados de recuperación y acta o informe de cierre.
- Consolidar las lecciones aprendidas mediante reuniones posteriores al cierre del incidente, análisis de causas, identificación de controles que fallaron o requieren fortalecimiento y definición de acciones de mejora, registrándolas en la herramienta institucional. Realizar después del cierre de los incidentes significativos o cuando el análisis determine oportunidades de mejora. Evidencia: actas de lecciones aprendidas, análisis de causa raíz, acciones de mejora y registros en la herramienta institucional.
- Construir y mantener una base de conocimiento de incidentes mediante el registro estructurado de tipologías, causas, indicadores de compromiso, activos afectados, técnicas utilizadas, acciones de contención, recuperación y medidas preventivas. Actualizar después del cierre de incidentes y consultar durante el análisis de eventos o incidentes similares. Evidencia: base de conocimiento, registros históricos, indicadores y referencias de incidentes relacionados.
- Escalar los incidentes mediante una matriz de escalamiento que establezca criterios de severidad, destinatarios, canales, tiempos y condiciones para la notificación interna o externa. Aplicar inmediatamente cuando el incidente alcance los criterios definidos de impacto, criticidad, afectación legal, contractual o reputacional. Evidencia: matriz de escalamiento, registros de notificación, correos o

tickets y confirmaciones de recepción.

- Mantener actualizados los contactos de grupos de interés y comunidades especializadas en seguridad mediante un directorio institucional que incluya canales de comunicación y condiciones de contacto, considerando entidades como ColCERT, CSIRT Gobierno, Centro Cibernético Policial, mesas de infraestructura crítica y asociaciones especializadas. Verificar como mínimo anualmente y actualizar ante cambios en los canales o entidades de contacto; activar la comunicación cuando la naturaleza del incidente requiera apoyo externo. Evidencia: directorio actualizado, registros de revisión, comunicaciones y solicitudes de asistencia.
- Aplicar criterios estandarizados para clasificar y gestionar los incidentes mediante categorías de clasificación, prioridad, impacto, mecanismo de contención, erradicación, recuperación y tiempos de respuesta diferenciados por criticidad, alineados con la guía vigente del MinTIC. Utilizar estos criterios desde el registro inicial y actualizarlos durante el ciclo de vida cuando cambie la severidad o impacto. Evidencia: matriz de clasificación, registros de incidentes, tiempos de atención, bitácoras y reportes de cumplimiento.

La SIDT

- Coordinar la atención técnica de los incidentes mediante la activación del procedimiento de respuesta, asignación de actividades, priorización de recursos, contención y recuperación de los servicios afectados. Aplicar inmediatamente después de recibir un incidente confirmado o escalado y mantener seguimiento hasta su estabilización y cierre. Evidencia: tickets, bitácoras técnicas, registros de acciones, comunicaciones y reportes de cierre.

- Gestionar los eventos de seguridad mediante herramientas de monitoreo, correlación y análisis de registros, aplicando reglas de detección y criterios de priorización para determinar si corresponden a incidentes de seguridad o privacidad. Realizar monitoreo continuo y clasificar los eventos conforme a los criterios institucionales. Evidencia: alertas, logs, casos de monitoreo, análisis de eventos y registros de clasificación.
- Informar los incidentes a los niveles administrativos correspondientes mediante los canales y formatos establecidos, comunicando como mínimo la naturaleza del incidente, severidad, impacto, activos afectados, acciones ejecutadas y estado de atención. Realizar la notificación dentro de los tiempos definidos según la criticidad y actualizarla ante cambios relevantes. Evidencia: informes ejecutivos, comunicaciones, tickets, actas y registros de escalamiento.
- Recolectar y preservar la evidencia digital mediante procedimientos de adquisición, identificación, integridad, almacenamiento, control de acceso y trazabilidad, manteniendo la cadena de custodia cuando sea requerida. Realizar la recolección durante la atención del incidente y antes de ejecutar acciones que puedan alterar o eliminar evidencia relevante. Evidencia: imágenes o archivos de evidencia, hashes, registros de adquisición, cadena de custodia, logs y repositorio controlado.

Funcionarios y terceros de la entidad

- Reportar los eventos, incidentes o situaciones anormales mediante los canales institucionales autorizados, proporcionando información sobre el evento observado, activo afectado, fecha y hora, descripción y evidencias disponibles, y evitando realizar acciones que puedan alterar

la evidencia. Realizar el reporte inmediatamente después de identificar la situación y escalarlo cuando se presenten nuevos elementos que modifiquen su impacto o alcance. Evidencia: ticket, correo, formulario de reporte, registro en mesa de servicio y evidencias adjuntas.

- Clasificar y direccionar los reportes recibidos mediante las categorías y criterios establecidos, remitiéndolos a la SIDT y/o Seguridad de la Información según su naturaleza, impacto y criticidad. Aplicar al momento de registrar cada reporte y actualizar la clasificación cuando el análisis técnico determine que corresponde a un incidente. Evidencia: registro del reporte, categoría asignada, ticket de escalamiento y trazabilidad del tratamiento.

8.7.2. Evaluación de eventos de seguridad

Control Asociado en el MSPI A.5.26

Evaluar los eventos de seguridad presentados en la entidad, valorarlos y decidir si se clasifica como incidente de seguridad y privacidad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Evaluar los eventos de seguridad mediante el análisis conjunto de las alertas, registros, activos afectados, comportamiento observado e impacto potencial, aplicando los criterios institucionales para determinar si el evento constituye un incidente de seguridad o privacidad de la información. Realizar la evaluación durante el análisis inicial de cada evento y actualizarla cuando se obtenga información adicional que modifique su impacto o naturaleza. Evidencia: registros de eventos, análisis de evaluación, criterios aplicados y trazabilidad de la decisión.
- Evaluar y clasificar los incidentes de seguridad y privacidad mediante la valoración de su impacto, criticidad, activos afectados, información

comprometida, alcance y nivel de riesgo, aplicando la matriz o Tabla de Impacto de Incidentes establecida por la entidad. Realizar la clasificación al momento de confirmar el incidente y actualizarla cuando cambien las condiciones, alcance o impacto. Evidencia: registro del incidente, matriz de clasificación, Tabla de Impacto aplicada y registros de actualización.

- Implementar un mecanismo especializado de monitoreo y gestión de incidentes mediante la asignación de funciones para monitorear eventos, analizar alertas, clasificar incidentes, realizar notificaciones, coordinar el tratamiento y efectuar seguimiento hasta el cierre. Operar de manera continua y activar el esquema de atención de acuerdo con la criticidad y severidad de cada incidente. Evidencia: matriz de roles, registros de monitoreo, tickets, alertas, escalamiento y reportes de gestión.
- Categorizar los incidentes mediante la aplicación de la Tabla de Impacto de Incidentes, considerando criterios como afectación a la confidencialidad, integridad y disponibilidad, número de activos o usuarios afectados, criticidad del servicio, alcance y consecuencias para la entidad. Aplicar durante la clasificación inicial y reevaluar ante cambios significativos en el impacto o alcance. Evidencia: Tabla de Impacto diligenciada, valoración del incidente, registro de severidad y trazabilidad de cambios.

La SIDT

- Aplicar los procedimientos, lineamientos y requisitos normativos institucionales para la gestión de incidentes mediante las etapas de identificación, registro, análisis, clasificación, contención, erradicación, recuperación, cierre y lecciones aprendidas. Utilizar durante todo el ciclo de vida de cada incidente y actualizar su aplicación cuando se modifiquen los criterios o procedimientos vigentes. Evidencia: procedimientos

vigentes, tickets, bitácoras, registros de tratamiento y reportes de cierre.

- Clasificar los eventos e incidentes mediante la aplicación de las categorías, criterios de severidad, impacto y tipología establecidos en los documentos y procedimientos institucionales. Realizar la clasificación durante el análisis inicial y actualizarla cuando la investigación determine una nueva condición o nivel de afectación. Evidencia: registros de eventos, matriz de clasificación, categorización asignada y trazabilidad de modificaciones.
- Gestionar y responder los eventos confirmados como incidentes mediante acciones de contención, análisis técnico, erradicación, recuperación y validación de los servicios afectados, siguiendo los procedimientos y tiempos establecidos según su criticidad. Activar inmediatamente después de la confirmación del incidente y mantener las acciones hasta verificar su contención, recuperación y cierre. Evidencia: tickets, bitácoras técnicas, registros de acciones ejecutadas, resultados de recuperación y acta o informe de cierre.
- Analizar, validar y documentar cada incidente mediante el registro cronológico de su identificación, clasificación, activos afectados, evidencias recolectadas, acciones ejecutadas, impacto, comunicaciones, escalamiento, recuperación y resultado final. Mantener la trazabilidad durante todo el ciclo de vida del incidente y completar la documentación antes de su cierre formal. Evidencia: expediente del incidente, bitácora, evidencias digitales, comunicaciones, registros de escalamiento y reporte de cierre.
- Incorporar las lecciones aprendidas en la base de conocimiento mediante el registro de causas, vulnerabilidades explotadas, indicadores de compromiso, controles involucrados, acciones efectivas y oportunidades

de mejora identificadas durante el análisis posterior al incidente. Realizar después del cierre de cada incidente significativo o cuando se identifiquen hallazgos reutilizables para otros casos. Evidencia: base de conocimiento actualizada, análisis de causa raíz, registro de lecciones aprendidas y acciones de mejora.

8.7.3. Respuesta ante incidentes de seguridad de la información

Control Asociado en el MSPI A.5.27

Gestionar los incidentes identificados para minimizar su impacto y restaurar las operaciones. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Registrar y gestionar la respuesta a cada incidente de seguridad y privacidad mediante un formato o herramienta institucional que consolide, como mínimo, el tipo de incidente, activo de información afectado, criticidad, debilidades o vulnerabilidades identificadas, personas involucradas en el tratamiento, actividades ejecutadas, duración de la atención y estado del incidente. Diligenciar durante todo el ciclo de gestión y actualizar hasta su cierre formal. Evidencia: registro o ticket del incidente, bitácora de atención y reporte de cierre.
- Documentar las debilidades de seguridad que hayan causado o contribuido al incidente mediante el análisis técnico de configuraciones, vulnerabilidades, controles existentes y condiciones que facilitaron su ocurrencia. Realizar durante el análisis del incidente y validar los hallazgos antes del cierre. Evidencia: análisis técnico, resultados de evaluación de vulnerabilidades, evidencias digitales y registro de causas identificadas.
- Asignar y registrar las personas que intervienen en el tratamiento del

incidente mediante la designación de roles para primer respondiente, análisis técnico, coordinación, comunicación y recuperación, de acuerdo con la severidad y naturaleza del incidente. Realizar al inicio del tratamiento y actualizar ante cambios en las necesidades de atención. Evidencia: registro del incidente, matriz de roles, asignaciones en tickets y bitácora de actividades.

- Registrar las actividades de tratamiento y respuesta mediante una bitácora cronológica que permita identificar las acciones de contención, análisis, erradicación, recuperación, comunicación y validación ejecutadas. Actualizar durante la atención y completar antes del cierre del incidente. Evidencia: bitácora, tickets, registros técnicos, comunicaciones y evidencias de las acciones ejecutadas.
- Medir y registrar la duración de la atención mediante el registro de fecha y hora de detección, reporte, inicio de tratamiento, contención, recuperación y cierre, comparando los tiempos obtenidos con los ANS o tiempos de respuesta definidos según la criticidad. Aplicar en cada incidente y consolidar periódicamente para identificar desviaciones y oportunidades de mejora. Evidencia: registros de fecha y hora, indicadores de atención, reportes de cumplimiento y análisis de tiempos.
- Actualizar el estado del incidente mediante estados controlados de Abierto, cuando el tratamiento no haya concluido o persistan acciones pendientes, y Cerrado, cuando las acciones de tratamiento hayan finalizado y se haya validado la recuperación o mitigación correspondiente. Actualizar durante cada etapa del ciclo de atención y realizar el cierre únicamente después de la validación establecida. Evidencia: historial de estados del ticket, criterios de cierre, validación de recuperación y reporte de cierre.
- Documentar las respuestas y soluciones aplicadas en la base de

conocimiento de incidentes mediante el registro de tipología, causa, impacto, indicadores de compromiso, acciones de contención, erradicación y recuperación, resultados obtenidos y recomendaciones. Actualizar después del cierre de cada incidente significativo o cuando la información pueda ser reutilizada para atender eventos similares. Evidencia: registro en la base de conocimiento, artículos técnicos y referencias cruzadas con los incidentes relacionados.

- Notificar los incidentes a los entes de control o autoridades competentes mediante los canales, formatos y plazos establecidos en los procedimientos institucionales y requisitos legales o contractuales aplicables. Realizar la notificación cuando la naturaleza, impacto o regulación del incidente así lo determine y conservar la trazabilidad de la comunicación. Evidencia: comunicaciones oficiales, formularios de notificación, acuses de recibo y registros del expediente del incidente.
- Aplicar medidas de contención mediante el aislamiento de activos, bloqueo de cuentas, restricción de comunicaciones, suspensión de servicios o implementación de controles temporales, seleccionando las acciones de acuerdo con el tipo, criticidad e impacto del incidente. Ejecutar inmediatamente después de confirmar la necesidad de contención y validar posteriormente que la medida no genere impactos no controlados sobre otros servicios. Evidencia: órdenes de cambio, configuraciones, logs, registros de aislamiento y resultados de validación.
- Recolectar y preservar la evidencia digital mediante procedimientos de adquisición, identificación, integridad, almacenamiento seguro y control de acceso, utilizando mecanismos de hash y cadena de custodia cuando sean necesarios. Realizar durante la investigación y antes de ejecutar acciones que puedan modificar o eliminar información relevante.

Evidencia: archivos o imágenes de evidencia, hashes, registros de adquisición, cadena de custodia y bitácoras.

- Comunicar el incidente a las partes interesadas internas y externas mediante una matriz de comunicaciones que establezca destinatarios, canales, contenido mínimo, nivel de autorización y tiempos de notificación. Aplicar de acuerdo con la criticidad, impacto y obligaciones legales, regulatorias o contractuales del incidente. Evidencia: matriz de comunicaciones, correos, comunicados, tickets, actas y registros de notificación.
- Coordinar la respuesta con las partes internas y externas mediante canales de atención, reuniones de seguimiento, mecanismos de escalamiento y asignación de acciones, manteniendo una única trazabilidad de las decisiones y actividades ejecutadas. Activar cuando el incidente requiera participación de varias dependencias, proveedores o entidades externas y mantener hasta su estabilización o cierre. Evidencia: actas, tickets, registros de escalamiento, planes de acción y comunicaciones.
- Analizar la causa raíz mediante técnicas de análisis como línea de tiempo, correlación de eventos, análisis de vulnerabilidades, revisión de configuraciones y metodología de causa raíz, diferenciando causas directas, contribuyentes y condiciones subyacentes. Realizar para incidentes significativos, recurrentes o aquellos que evidencien fallas de controles, antes del cierre definitivo o dentro del análisis posterior. Evidencia: análisis de causa raíz, línea de tiempo, resultados técnicos y conclusiones del incidente.
- Identificar y gestionar las vulnerabilidades y debilidades de los controles relacionadas con la causa del incidente mediante el registro de hallazgos, valoración del riesgo, definición de acciones correctivas, asignación de

plazos y verificación de su implementación. Aplicar después de identificar la causa o debilidad y realizar seguimiento hasta validar la remediación. Evidencia: matriz de vulnerabilidades, tickets de remediación, planes de tratamiento, resultados de pruebas y evidencias de cierre.

- Asignar y formalizar los roles de primer respondiente y vocero oficial mediante una matriz de responsabilidades y criterios de activación según la criticidad y naturaleza del incidente. Definir antes de la atención y activar los roles correspondientes en cada incidente que requiera respuesta coordinada o comunicación oficial. Evidencia: matriz de roles, procedimientos, registros de activación, actas y comunicaciones oficiales.
- Informar a los propietarios de los activos afectados mediante los canales institucionales definidos, comunicando la naturaleza del incidente, activo comprometido, impacto identificado, estado de atención, medidas de contención y acciones de remediación o recuperación ejecutadas. Realizar la notificación de acuerdo con la criticidad y durante las etapas relevantes del tratamiento, manteniendo actualizaciones hasta el cierre cuando corresponda. Evidencia: comunicaciones, tickets, informes de incidente, acuses de recibo y registros de seguimiento.

8.7.4. Aprendizaje a partir de incidentes de seguridad

Control Asociado en el MSPI A.5.28

Mantener y utilizar la base de datos de conocimiento para reducir la posibilidad o el impacto de futuros incidentes, utilizar las lecciones aprendidas para los planes de respuesta a los incidentes de seguridad y privacidad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Cuantificar y hacer seguimiento a los incidentes de seguridad y

privacidad de la información mediante un registro centralizado que consolide, como mínimo, tipo de incidente, cantidad, volumen de eventos, activos afectados, tiempo de atención y costos asociados; actualizar la información durante la gestión de cada incidente y consolidarla periódicamente para su análisis. Evidencia: registro de incidentes, indicadores, reportes estadísticos y análisis de costos.

- Analizar la información consolidada de los incidentes mediante criterios de recurrencia, frecuencia, impacto, criticidad, activos afectados y costos, como mínimo durante las revisiones periódicas de los indicadores y después de incidentes de alto impacto, para identificar tendencias e incidentes recurrentes. Evidencia: informes de análisis, tendencias, clasificación de recurrencia y registros de incidentes relacionados.
- Incorporar las lecciones aprendidas de los incidentes en los contenidos de formación y concienciación mediante casos reales, escenarios de ataque, medidas preventivas y buenas prácticas, posterior al cierre de incidentes relevantes y durante la actualización periódica del plan de sensibilización. Evidencia: material de capacitación actualizado, registros de asistencia, evaluaciones y plan de sensibilización.
- Actualizar la base de conocimiento de incidentes mediante el registro estructurado de amenazas, vulnerabilidades, causas, patrones, activos afectados, escenarios, controles aplicados y oportunidades de mejora, posterior al análisis y cierre de cada incidente que genere información reutilizable. Evidencia: base de conocimiento, análisis de incidentes, registros de vulnerabilidades y acciones de mejora.
- Registrar y evaluar las necesidades de controles adicionales o mejoras mediante el análisis de las causas y condiciones que favorecieron cada incidente, al finalizar la investigación y durante el seguimiento de las acciones correctivas, priorizando aquellas que reduzcan la frecuencia o

recurrencia. Evidencia: análisis de causa, plan de tratamiento, solicitudes de cambio y resultados de implementación.

- Estimar y registrar los daños y costos asociados a incidentes mediante la consolidación de costos de recuperación, indisponibilidad, afectación operativa, pérdida o exposición de información y recursos utilizados, durante el cierre y análisis posterior de incidentes de impacto significativo. Evidencia: informe de impacto, registros de costos y análisis posterior al incidente.
- Actualizar los contenidos de sensibilización mediante la incorporación de comportamientos observados, errores recurrentes, técnicas de ataque y medidas preventivas identificadas durante los incidentes, como resultado de las lecciones aprendidas y en cada ciclo de actualización del plan. Evidencia: contenidos actualizados, plan de sensibilización y registros de capacitación.
- Revisar y actualizar los procedimientos y políticas de seguridad de la información mediante la comparación entre las actividades ejecutadas durante el incidente y los controles documentados, cuando se identifiquen brechas, cambios necesarios o lecciones aprendidas relevantes. Evidencia: versiones actualizadas, control de cambios, actas de revisión y registros de aprobación.
- Actualizar los registros de riesgos y causas de riesgo mediante la incorporación de nuevas amenazas, vulnerabilidades, causas y escenarios identificados durante el análisis de incidentes, cuando los resultados modifiquen la valoración o tratamiento de los riesgos existentes. Evidencia: matriz de riesgos actualizada, análisis de riesgos y plan de tratamiento.
- Mejorar el procedimiento de gestión de incidentes mediante la incorporación de las lecciones aprendidas, tiempos de respuesta,

dificultades encontradas, actividades efectivas y oportunidades de optimización, posterior a incidentes significativos y durante las revisiones periódicas del procedimiento. Evidencia: procedimiento actualizado, control de cambios y análisis posterior al incidente.

- Identificar y registrar acciones preventivas mediante la evaluación de las causas y condiciones que originaron o facilitaron los incidentes, antes del cierre de los incidentes relevantes y durante el seguimiento de las acciones correctivas, estableciendo medidas orientadas a reducir su probabilidad de ocurrencia. Evidencia: plan de acciones, registros de seguimiento y resultados de verificación.
- Identificar y priorizar los activos de información más vulnerables mediante el análisis de recurrencia, criticidad, vulnerabilidades, exposición e incidentes asociados, durante las revisiones de riesgos y después de incidentes que involucren activos críticos. Evidencia: inventario de activos priorizados, matriz de riesgos y análisis de vulnerabilidades.
- Correlacionar los eventos e incidentes registrados mediante el análisis de fechas, activos, indicadores de compromiso, técnicas utilizadas, vectores de ataque y comportamientos observados, durante la investigación de incidentes y en los análisis periódicos de tendencias, para identificar posibles patrones de ataques informáticos. Evidencia: análisis de correlación, líneas de tiempo, IOCs, reportes de inteligencia y registros de incidentes relacionados.
- Documentar escenarios de incidentes mediante la descripción de vectores de ataque, activos afectados, condiciones de ocurrencia, impacto, controles existentes y posibles respuestas, a partir de incidentes reales y durante los ejercicios de simulación o pruebas de respuesta. Evidencia: escenarios documentados, resultados de ejercicios

y planes de respuesta actualizados.

- Monitorear los riesgos de seguridad y privacidad de la información mediante el seguimiento de indicadores, vulnerabilidades, incidentes, amenazas, cambios tecnológicos y resultados de controles, de forma continua y durante las revisiones periódicas de riesgos, ajustando su valoración cuando se presenten nuevas condiciones. Evidencia: tableros de monitoreo, indicadores, informes de riesgos y matrices actualizadas.

Registro de lecciones aprendidas

- Registrar cronológicamente los hechos ocurridos durante cada incidente mediante la documentación de fecha y hora de detección, identificación, clasificación, acciones ejecutadas, comunicaciones, recuperación y cierre, desde la identificación hasta el cierre formal del incidente. Evidencia: bitácora del incidente, tickets, registros de eventos y reporte de cierre.
- Verificar la aplicación de los procedimientos documentados mediante la comparación de las actividades ejecutadas con las etapas, controles y criterios establecidos para la gestión de incidentes, durante el análisis posterior y antes del cierre de incidentes relevantes. Evidencia: lista de verificación, análisis de cumplimiento y reporte de lecciones aprendidas.
- Identificar y documentar las medidas o acciones que hayan generado dificultades o impedido la recuperación mediante el análisis de su impacto sobre la contención, erradicación, recuperación o continuidad, durante el análisis posterior al incidente. Evidencia: análisis técnico, línea de tiempo, hallazgos y registro de oportunidades de mejora.
- Definir y registrar acciones correctivas mediante el análisis de causas raíz, vulnerabilidades y controles deficientes, posterior a incidentes relevantes y hasta verificar su implementación y efectividad. Evidencia:

plan de acción, tickets de remediación, resultados de pruebas y registros de cierre.

- Identificar y documentar las herramientas y recursos requeridos mediante el análisis de las limitaciones encontradas durante la detección, investigación, contención y recuperación, al finalizar incidentes significativos y durante la planificación de mejoras. Evidencia: informe de necesidades, plan de mejora, solicitudes de adquisición o configuración y pruebas realizadas.
- Comunicar y revisar las lecciones aprendidas con los propietarios de los activos afectados mediante reuniones, informes o comunicaciones formales que documenten el incidente, impacto, tratamiento, causas, resultados y acciones de mejora, posterior al cierre de incidentes relevantes y cuando se requiera coordinación para implementar acciones correctivas. Evidencia: actas, informes, comunicaciones y planes de acción.

La SIDT

- Cuantificar y hacer seguimiento a los incidentes de seguridad y privacidad que afecten la infraestructura tecnológica mediante una herramienta o registro centralizado que consolide tipo, volumen, frecuencia, activos afectados, criticidad, tiempos de atención y costos, actualizado durante la gestión de cada incidente y consolidado periódicamente. Evidencia: plataforma o registro de incidentes, indicadores, tableros y reportes periódicos.
- Documentar y mantener actualizada la base de conocimiento de incidentes mediante el registro de amenazas, vulnerabilidades, causas, activos afectados, indicadores de compromiso, patrones de ataque, escenarios, controles aplicados y oportunidades de mejora identificadas

durante las investigaciones, después del cierre de cada incidente relevante y cuando se genere conocimiento reutilizable para prevenir o responder a nuevos eventos. Evidencia: base de conocimiento, informes técnicos, análisis de causa raíz, registros de vulnerabilidades, IOCs y acciones de mejora.

8.7.5. Informe de eventos de seguridad de la información

Control Asociado en el MSPI A.6.8

Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que se puedan identificar por el personal. Por lo tanto, se desarrollarán las siguientes actividades:

- Establecer y documentar el procedimiento para el reporte de posibles eventos de seguridad y privacidad mediante un flujo que incluya identificación, registro, clasificación, escalamiento y atención, incorporando los responsables de cada actividad, canales autorizados de comunicación, tiempos de respuesta y criterios de clasificación; revisarlo como mínimo una vez al año y actualizarlo cuando se presenten cambios organizacionales, tecnológicos, normativos o derivados de incidentes. Evidencia: procedimiento aprobado, matriz de clasificación, directorio de contactos, canales habilitados y registro de control de cambios.
- Implementar mecanismos para registrar los posibles eventos mediante formularios, mesa de servicios, correo institucional, plataforma de gestión de incidentes u otros canales autorizados, solicitando como mínimo fecha y hora, descripción del evento, activo o servicio afectado, información involucrada y datos de contacto del reportante; en cada reporte recibido y hasta su clasificación y cierre. Evidencia: tickets, formularios, correos, registros de la herramienta y bitácoras de atención.
- Clasificar los posibles eventos reportados mediante criterios definidos de tipo, impacto potencial, criticidad, afectación a la confidencialidad,

integridad o disponibilidad y posibilidad de constituir un incidente, durante la evaluación inicial y cada vez que se obtenga información que modifique su valoración. Evidencia: registro del evento, matriz de clasificación, valoración de impacto y trazabilidad de cambios.

- Socializar el procedimiento de reporte mediante capacitaciones, campañas de sensibilización, piezas comunicativas, intranet y otros medios institucionales, explicando los tipos de eventos que deben reportarse, los canales disponibles, la información requerida y los tiempos de comunicación; como mínimo durante el proceso de inducción y periódicamente de acuerdo con el plan de sensibilización, así como cuando se modifique el procedimiento o los canales. Evidencia: material divulgado, registros de capacitación, publicaciones, listas de asistencia y evaluaciones de conocimiento.
- Ejecutar ejercicios controlados de ingeniería social mediante campañas simuladas que reproduzcan escenarios como correos de phishing, solicitudes fraudulentas, enlaces maliciosos o suplantación, sin generar afectaciones reales a los sistemas o información, periódicamente y de acuerdo con el plan de ejercicios de seguridad. Evidencia: plan y autorización del ejercicio, escenarios utilizados, resultados y métricas de participación.
- Verificar el uso adecuado de los canales de reporte durante los ejercicios de ingeniería social mediante el seguimiento de las acciones realizadas por los participantes, incluyendo identificación del evento, reporte oportuno, canal utilizado y tiempo transcurrido entre la detección y el reporte; al finalizar cada ejercicio y mediante el análisis comparativo de resultados. Evidencia: registros de reportes, métricas de participación, tiempos de respuesta y resultados consolidados.
- Implementar acciones de mejora a partir de los resultados de los

ejercicios mediante la identificación de comportamientos recurrentes, deficiencias en el conocimiento de los canales, tiempos de reporte y oportunidades de fortalecimiento, posterior a cada ejercicio y hasta verificar la implementación de las acciones definidas. Evidencia: informe de resultados, plan de mejora, registros de sensibilización y resultados de ejercicios posteriores.

8.7.6. Registro

Control Asociado en el MSPI A.8.15

Para registrar eventos, generar pruebas, garantizar la integridad de información de registro, prevenir contra el acceso no autorizado, identificar los eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y apoyar las investigaciones. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Implementar controles para proteger los registros almacenados en bases de datos, registros de transacciones (Logs) y registros de auditoría (Audit Logs), mediante lineamientos, procedimientos e instructivos que establezcan controles de acceso, integridad, trazabilidad, almacenamiento, retención, respaldo y disposición; aplicar estos controles durante todo el ciclo de vida de los registros y revisarlos ante cambios tecnológicos, normativos o de riesgo. Evidencia: lineamientos, procedimientos, configuraciones de seguridad, matrices de acceso, registros de revisión y auditorías.
- Configurar y administrar los sistemas de almacenamiento y gestión de registros mediante controles que permitan conservar, consultar, recuperar, identificar, retener y disponer de la información de acuerdo con su clasificación y requisitos aplicables; verificar su funcionamiento durante la operación y mediante pruebas periódicas de recuperación y

disposición. Evidencia: configuraciones, inventarios, políticas de almacenamiento, resultados de pruebas y registros de operación.

- Conservar la legibilidad y accesibilidad de los registros durante todo el período de retención mediante formatos sostenibles, mecanismos de migración, conversión o actualización tecnológica y validaciones de integridad, antes de que una tecnología, formato o medio de almacenamiento quede obsoleto y durante el período de retención. Evidencia: inventario de formatos y medios, planes de migración, registros de conversión y pruebas de lectura.
- Recuperar y validar los registros mediante procedimientos de búsqueda, restauración y exportación que permitan obtener la información requerida en el tiempo y formato definidos según su finalidad, criticidad y requisitos legales, reglamentarios o contractuales; realizar pruebas periódicas y cada vez que se requiera una recuperación formal. Evidencia: solicitudes de recuperación, registros de restauración, tiempos obtenidos, archivos recuperados y resultados de las pruebas.
- Identificar y clasificar los registros mediante un inventario que relacione fuente, tipo de registro, información contenida, clasificación, período de retención, ubicación y mecanismo de almacenamiento, actualizándolo cuando se creen, modifiquen o retiren fuentes de información y verificándolo periódicamente. Evidencia: inventario de registros, matriz de clasificación y registros de actualización.
- Ejecutar la disposición de los registros mediante métodos de eliminación o destrucción segura que impidan su recuperación no autorizada, de acuerdo con el período de retención y las autorizaciones aplicables; realizarla una vez cumplido el período de retención y confirmada la inexistencia de requerimientos legales, administrativos, contractuales o de auditoría que obliguen a conservarlos. Evidencia: actas o certificados

de disposición, registros de eliminación, evidencias de borrado seguro y autorizaciones correspondientes.

- Documentar y aplicar los procedimientos para retención, almacenamiento, manejo y disposición de registros electrónicos mediante criterios alineados con el Programa de Gestión Documental y los requisitos legales, reglamentarios y contractuales aplicables; revisarlos periódicamente y actualizarlos cuando se modifiquen dichos requisitos o los procesos institucionales. Evidencia: procedimientos aprobados, matriz de requisitos, control de cambios y registros de aplicación.
- Implementar el programa de retención mediante una matriz que relacione cada tipo de registro electrónico con su período de conservación, condición de inicio del término, medio de almacenamiento y disposición final; actualizarlo ante cambios en las tablas de retención, requisitos legales, procesos o sistemas de información. Evidencia: programa o matriz de retención, tablas de retención documental y registros de actualización.
- Mantener un inventario de las fuentes de información mediante la identificación de bases de datos, aplicaciones, sistemas, dispositivos, plataformas, servicios tecnológicos y repositorios que generen o almacenen registros, relacionándolos con el inventario y clasificación de activos de información; actualizarlo ante la incorporación, modificación o retiro de activos. Evidencia: inventario de fuentes, inventario de activos y matriz de correspondencia.
- Aplicar los períodos de retención y condiciones de almacenamiento mediante controles que consideren requisitos estatutarios, reglamentarios, contractuales, necesidades de las actividades misionales y lineamientos del Programa de Gestión Documental; verificar su

cumplimiento durante las revisiones periódicas de los registros y ante cambios regulatorios o contractuales. Evidencia: matriz de requisitos, registros de retención, informes de verificación y resultados de auditoría.

- Proteger los registros de eventos generados por el hardware y software de la infraestructura de seguridad mediante almacenamiento seguro, control de acceso basado en privilegios, autenticación, protección contra modificación o eliminación no autorizada, respaldo y mecanismos de monitoreo; mantener estos controles durante todo el período de conservación y verificar periódicamente su integridad y disponibilidad. Evidencia: configuraciones de almacenamiento y acceso, logs, registros de auditoría, respaldos, controles de integridad y resultados de verificación.
- Restringir el acceso a los registros de seguridad mediante cuentas individuales, permisos mínimos, grupos autorizados y mecanismos de autenticación y trazabilidad, manteniendo los accesos únicamente durante el tiempo requerido y revisándolos periódicamente. Evidencia: matriz de accesos, registros de autenticación, permisos configurados y reportes de revisión.
- Reportar los eventos o incidentes relacionados con pérdida, destrucción, falsificación, acceso no autorizado o divulgación no autorizada de registros mediante los canales institucionales de gestión de incidentes, incluyendo fecha, registro afectado, tipo de evento, evidencia disponible e impacto identificado; realizar el reporte inmediatamente después de su detección y efectuar seguimiento hasta su cierre. Evidencia: ticket o reporte de incidente, comunicaciones, logs, evidencias digitales, análisis y registro de cierre.

Funcionarios y terceros

- Aplicar los lineamientos del Programa de Gestión Documental mediante el cumplimiento de los períodos de retención, condiciones de almacenamiento, manejo, acceso y disposición establecidos para los registros e información electrónica, durante todo el ciclo de vida de la información y cada vez que se consulte, modifique, transfiera, archive o disponga un registro. Evidencia: registros de gestión documental, controles de acceso, trazabilidad de consultas o modificaciones y soportes de disposición.

8.7.7. Actividades de monitoreo

Control Asociado en el MSPI A.8.16

Monitorear las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y tomar medidas apropiadas de forma oportuna para evaluar posibles incidentes de seguridad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Monitorear continuamente los eventos generados por sistemas de información, infraestructura, aplicaciones y redes mediante la herramienta FALCON, herramienta de registro, correlación y análisis de eventos de seguridad, priorizando aquellos que puedan afectar la confidencialidad, integridad o disponibilidad; mantener el monitoreo activo de forma permanente y ajustar las fuentes cuando se incorporen, modifiquen o retiren activos. Evidencia: registros de monitoreo, eventos recolectados, tableros, reglas de correlación y reportes.
- Generar y escalar alertas de seguridad mediante reglas configuradas en las herramientas de monitoreo y canales institucionales de notificación, incluyendo información sobre activo afectado, tipo de evento, fecha, hora, severidad y evidencia disponible; de manera inmediata cuando se

superen los umbrales definidos o se identifiquen comportamientos anómalos. Evidencia: alertas, tickets, correos o mensajes de notificación y registros de escalamiento.

- Establecer y mantener líneas base de comportamiento mediante la recopilación histórica de métricas de red, sistemas, aplicaciones e infraestructura, diferenciando períodos normales y de alta demanda y considerando variables como volumen de tráfico, conexiones, consumo de recursos, latencia, autenticaciones y transacciones; actualizarlas periódicamente y ante cambios relevantes de arquitectura, capacidad o comportamiento operativo. Evidencia: líneas base aprobadas, métricas históricas, dashboards, informes de análisis y registros de actualización.
- Detectar terminaciones no planificadas de procesos o aplicaciones mediante la correlación de registros de sistema, eventos de servicios, códigos de error y estados de ejecución con la línea base definida; generar alerta cuando se identifiquen interrupciones fuera de las ventanas autorizadas. Evidencia: logs de sistema, alertas, tickets y análisis del evento.
- Detectar y analizar actividad asociada con malware o comunicaciones con direcciones IP, dominios o indicadores de compromiso conocidos mediante herramientas de protección de endpoints, análisis de tráfico, inteligencia de amenazas y correlación con fuentes de reputación; generar alertas ante coincidencias o comportamientos compatibles con actividad maliciosa. Evidencia: alertas, IOCs, registros de conexiones, resultados de análisis y reportes de inteligencia.
- Identificar características asociadas con ataques conocidos mediante reglas de detección, firmas, indicadores de comportamiento y análisis de anomalías para eventos como denegación de servicio, explotación de vulnerabilidades o desbordamiento de memoria; aplicar las reglas de

detección continuamente y actualizarlas cuando se incorporen nuevas amenazas o técnicas de ataque. Evidencia: reglas de detección, alertas, firmas actualizadas, registros de eventos y análisis técnicos.

- Detectar comportamientos inusuales de sistemas y aplicaciones mediante análisis de procesos, llamadas, autenticaciones, ejecución de comandos, uso de protocolos y cambios respecto de la línea base, incluyendo comportamientos como registro de pulsaciones, inyección de procesos o desviaciones de protocolos; generar alertas cuando se superen los criterios de anomalía establecidos. Evidencia: registros de eventos, alertas, análisis de comportamiento y resultados de investigación.
- Monitorear cuellos de botella y sobrecargas mediante métricas de utilización de CPU, memoria, almacenamiento, ancho de banda, colas de red, latencia, pérdida de paquetes y fluctuaciones de tráfico; realizar seguimiento continuo y generar alertas cuando los valores superen los umbrales definidos. Evidencia: métricas de capacidad, dashboards, alertas, informes de desempeño y registros de acciones correctivas.
- Detectar accesos no autorizados o intentos de acceso mediante la correlación de autenticaciones exitosas y fallidas, privilegios utilizados, ubicación, dispositivo, horario y recurso solicitado; generar alertas ante patrones incompatibles con las reglas de acceso o el comportamiento esperado. Evidencia: logs de autenticación, eventos del SIEM, alertas y registros de investigación.
- Detectar actividades de escaneo no autorizado mediante herramientas de análisis de red y aplicaciones que identifiquen barridos de puertos, enumeración de servicios, exploración de vulnerabilidades y patrones anómalos de solicitudes; generar alertas cuando la actividad no corresponda a pruebas o actividades previamente autorizadas.

Evidencia: registros de red, alertas, resultados de detección y autorizaciones de pruebas.

- Monitorear los intentos exitosos y fallidos de acceso a recursos protegidos mediante registros de autenticación y autorización de servicios como DNS, portales web, servidores, bases de datos y sistemas de archivos; correlacionar los eventos de forma continua para identificar patrones de acceso anómalos. Evidencia: logs, eventos SIEM, reportes de acceso y alertas.
- Analizar el comportamiento de usuarios y sistemas mediante la comparación de actividades actuales con perfiles, roles, horarios, recursos utilizados y líneas base previamente establecidos; generar alertas cuando se identifiquen desviaciones significativas o actividades incompatibles con el comportamiento esperado. Evidencia: perfiles de comportamiento, registros de actividad, alertas y análisis de anomalías.
- Monitorear el tráfico entrante y saliente de red, sistemas y aplicaciones mediante firewalls, IDS/IPS, WAF, herramientas de protección de endpoints y plataformas de análisis de eventos, registrando origen, destino, protocolo, puerto, volumen y resultado de las comunicaciones; mantener la captura de eventos de manera continua y revisar las alertas generadas según su criticidad. Evidencia: logs de red, reglas de seguridad, alertas y reportes de tráfico.
- Revisar periódicamente los archivos de configuración de componentes de red y sistemas críticos o administrativos mediante listas de verificación y comparación contra configuraciones base autorizadas, identificando modificaciones no aprobadas o desviaciones de seguridad; realizar la revisión con una periodicidad definida por criticidad y después de cambios relevantes. Evidencia: checklists, configuraciones comparadas, registros de cambios, hallazgos y acciones correctivas.

- Registrar y revisar las actividades realizadas sobre las herramientas de seguridad mediante los logs administrativos de antivirus, EDR, IDS/IPS, filtros web, firewalls, DLP y demás controles implementados; realizar seguimiento continuo y revisión periódica de las actividades administrativas y cambios de configuración. Evidencia: logs administrativos, registros de cambios, reportes de auditoría y revisiones efectuadas.
- Configurar las herramientas de monitoreo mediante umbrales, reglas de correlación, niveles de severidad y canales automáticos de notificación, utilizando consolas, correo electrónico, sistemas de mensajería o mecanismos equivalentes; ajustar las reglas periódicamente con base en la línea base y los resultados de los análisis para reducir falsos positivos sin disminuir la capacidad de detección. Evidencia: reglas configuradas, umbrales, historial de cambios, alertas y métricas de efectividad.
- Identificar y gestionar los falsos positivos mediante el análisis de las alertas descartadas, validación de las condiciones que las generaron y ajuste controlado de reglas, umbrales o exclusiones; realizar el análisis periódicamente y cada vez que se detecte una concentración significativa de falsos positivos. Evidencia: registro de falsos positivos, análisis de causa, ajustes realizados y comparación de indicadores antes y después del ajuste.

Seguridad de la Información

- Generar y gestionar alertas ante actividades anómalas mediante reglas de correlación y umbrales configurados en las plataformas de monitoreo, clasificando cada alerta según criticidad e impacto potencial y registrando las acciones requeridas para su tratamiento; atenderlas

según los tiempos establecidos y verificar la efectividad de las medidas implementadas. Evidencia: alertas, tickets, análisis, planes de acción y registros de cierre.

- Monitorear las actividades de las bases de datos mediante una plataforma de auditoría y monitoreo que registre accesos, consultas, modificaciones, eliminaciones, cambios de privilegios y actividades administrativas, integrando estos eventos con el SIEM institucional; mantener la captura activa y verificar periódicamente la recepción, integridad y disponibilidad de los registros en el SIEM. Evidencia: logs de bases de datos, configuración de auditoría, eventos SIEM, dashboards y pruebas de integración.
- Escalar las actividades que puedan representar un riesgo para la seguridad mediante tickets, alertas o comunicaciones formales que incluyan activo afectado, actividad detectada, usuario o cuenta involucrada, fecha, hora, impacto potencial y evidencia disponible; realizar el escalamiento durante la evaluación del evento y actualizarlo cuando cambie su criticidad o impacto. Evidencia: tickets, comunicaciones, alertas, análisis y trazabilidad del escalamiento.
- Validar las actividades escaladas mediante la comparación con las funciones autorizadas, permisos asignados, cambios aprobados y comportamiento esperado, determinando si corresponden a una actividad legítima o a un evento anómalo; realizar la validación durante el análisis inicial y documentar la decisión adoptada. Evidencia: matriz de permisos, solicitudes de cambio, registros de actividad, análisis y decisión documentada.
- Bloquear actividades identificadas como no autorizadas o incompatibles con las funciones permitidas mediante reglas de firewall, EDR, IAM, bloqueo de cuentas, aislamiento de equipos u otros controles técnicos,

cuando el análisis determine un riesgo para la confidencialidad, integridad o disponibilidad y de acuerdo con los criterios de respuesta establecidos. Evidencia: registros de bloqueo, cambios de configuración, tickets, logs y validación posterior.

- Registrar y comunicar los riesgos, acciones y medidas de mitigación mediante informes o tickets que consoliden el evento, impacto, controles aplicados, riesgos residuales y acciones requeridas, durante la gestión del evento y hasta verificar la implementación de las medidas acordadas. Evidencia: informes, tickets, planes de tratamiento, registros de seguimiento y validaciones.
- Analizar las comunicaciones con IP, dominios y otros indicadores asociados con malware o servidores de comando y control mediante herramientas de reputación, inteligencia de amenazas, EDR y análisis de tráfico; realizar la revisión ante cada alerta y durante la investigación de eventos relacionados. Evidencia: IOCs, consultas de reputación, registros de conexión, alertas y análisis técnicos.
- Investigar las características de ataques conocidos mediante correlación de eventos, análisis de tráfico, comportamiento de procesos y comparación con indicadores y técnicas de ataque conocidas, incluyendo denegación de servicio, desbordamiento de memoria, registro de pulsaciones e inyección de procesos; realizar la revisión durante cada investigación en la que exista sospecha de actividad maliciosa. Evidencia: análisis técnico, eventos correlacionados, IOCs, resultados de investigación y reporte del incidente.
- Capacitar al personal mediante ejercicios prácticos y sesiones de formación orientadas a la interpretación de alertas, criterios de escalamiento, identificación de falsos positivos y aplicación del procedimiento de respuesta; realizar la formación durante la inducción

y periódicamente conforme al plan de capacitación, reforzándola después de cambios relevantes o incidentes significativos. Evidencia: material de capacitación, registros de asistencia, evaluaciones y resultados de ejercicios.

8.7.8. Sincronización de reloj

Control Asociado en el MSPI A.8.17

Permitir correlación y análisis de eventos relacionados con seguridad y otros datos registrados y apoyar investigaciones sobre incidentes de seguridad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Documentar los requisitos técnicos para la sincronización de relojes mediante una matriz o procedimiento que especifique la fuente oficial de tiempo, protocolo de sincronización, servidores de referencia, frecuencia de actualización, tolerancia de desviación, mecanismos de monitoreo y acciones ante pérdida de sincronización; revisarlos y actualizarlos cuando se incorporen o modifiquen servidores, sistemas, equipos o servicios tecnológicos. Evidencia: procedimiento, matriz de requisitos, diagramas de arquitectura y registros de actualización.
- Sincronizar los relojes de servidores, sistemas de procesamiento de información, equipos y servicios tecnológicos con la escala de tiempo internacional UTC mediante NTP versión 4 y fuentes de tiempo previamente autorizadas, configurando los servidores y dispositivos para realizar actualizaciones automáticas y validar la desviación respecto de la fuente de referencia; mantener la sincronización de forma continua y generar alertas ante pérdida de comunicación o desviaciones superiores al umbral definido. Evidencia: configuraciones NTP, registros de

sincronización, estado de los servicios de tiempo, logs y alertas.

- Verificar periódicamente la sincronización con la hora oficial de Colombia mediante la comparación de los relojes institucionales con la fuente oficial de tiempo proporcionada por el Instituto Nacional de Metrología, registrando la desviación identificada y aplicando correcciones cuando supere la tolerancia establecida; realizar las pruebas con la periodicidad definida y adicionalmente después de cambios en la infraestructura o ante eventos asociados a inconsistencias de tiempo. Evidencia: resultados de pruebas, registros de comparación, mediciones de desviación, acciones correctivas y reportes de verificación.
- Monitorear la disponibilidad y exactitud de la sincronización de tiempo mediante registros de NTP, estado de las fuentes de referencia, desviaciones detectadas y eventos generados por los sistemas, de forma continua y durante las revisiones periódicas de la infraestructura tecnológica. Evidencia: logs NTP, alertas, dashboards de monitoreo y reportes de revisión.
- Reportar los eventos o incidentes asociados con desviaciones, pérdida o alteración de la hora de servidores, sistemas, equipos o servicios tecnológicos mediante los canales institucionales de gestión de incidentes, incluyendo activo afectado, fecha y hora registrada, desviación identificada, impacto potencial y evidencia disponible; realizar el reporte inmediatamente después de su detección y efectuar seguimiento hasta su tratamiento y cierre. Evidencia: ticket o reporte de incidente, logs de tiempo, registros NTP, análisis técnico, acciones de corrección y evidencia de cierre.
- Investigar las inconsistencias de sincronización mediante el análisis de configuraciones NTP, disponibilidad de fuentes de tiempo, conectividad, registros de eventos y diferencias horarias entre sistemas relacionados,

cada vez que se detecte una desviación que pueda afectar la trazabilidad, correlación de eventos, autenticación, registros de auditoría o respuesta a incidentes. Evidencia: análisis técnico, comparación de tiempos, logs, diagnóstico y acciones correctivas.

8.8. Componente Política de Continuidad

8.8.1. Recolección de evidencia

Control Asociado en el MSPI A.5.29

Gestionar de manera eficaz y consistente la evidencia relacionada con incidentes de seguridad y privacidad de la información para efectos de acciones disciplinarias y legales. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

Gestión y preservación de evidencia digital

- Aplicar el procedimiento de gestión de evidencia digital mediante las etapas de aislamiento, identificación, recolección, examinación, análisis y reporte, utilizando las técnicas y controles establecidos en la normativa vigente y en los procedimientos institucionales; en cada incidente que requiera análisis o preservación de evidencia digital. Evidencia: procedimiento aplicado, registros de actuación, bitácoras, formularios y reporte final.
- Aislar la escena digital mediante la restricción de acceso a los equipos, sistemas, dispositivos y lugares relacionados con el incidente, evitando acciones que puedan modificar, sobrescribir o eliminar información relevante; inmediatamente después de determinar la necesidad de preservar evidencia y durante toda la fase de recolección. Evidencia: registro de aislamiento, fotografías, controles de acceso, bitácora y registro de fecha y hora.

- Identificar las fuentes potenciales de evidencia mediante el inventario de equipos, servidores, dispositivos de almacenamiento, registros, aplicaciones, servicios, cuentas, conexiones de red y medios volátiles relacionados con el incidente; antes de iniciar la adquisición de evidencia y actualizando el inventario cuando se identifiquen nuevas fuentes. Evidencia: inventario de fuentes, identificación de activos, fotografías y registros técnicos.
- Recolectar y examinar la información mediante herramientas forenses y procedimientos que preserven la integridad de los datos, priorizando los medios volátiles y posteriormente los medios no volátiles, de acuerdo con la naturaleza del incidente; durante la adquisición y antes de realizar análisis que puedan modificar la evidencia original. Evidencia: imágenes forenses, archivos adquiridos, registros de herramientas y bitácora de adquisición.
- Analizar la evidencia recolectada mediante técnicas de correlación de eventos, revisión de logs, análisis de archivos, memoria, procesos, conexiones, metadatos y demás elementos relevantes, manteniendo la trazabilidad entre cada hallazgo y su fuente; una vez finalizada la adquisición y durante la investigación del incidente. Evidencia: resultados de análisis, líneas de tiempo, indicadores de compromiso, hallazgos y registros técnicos.
- Reportar los resultados del análisis mediante un informe que documente hechos identificados, evidencia examinada, metodología utilizada, hallazgos, impacto, conclusiones y acciones recomendadas; al finalizar el análisis y antes del cierre formal del proceso de evidencia. Evidencia: informe técnico o forense, anexos de evidencia y registro de aprobación o cierre.
- Elementos para la recolección de información

- Mantener disponibles los elementos requeridos para la adquisición y preservación de evidencia mediante un inventario de equipos y materiales forenses, verificando su disponibilidad, integridad y estado operativo; antes de iniciar actividades de recolección y mediante revisiones periódicas del inventario. Evidencia: inventario, listas de verificación y registros de inspección.
- Utilizar dispositivos de recolección forense mediante herramientas y equipos que permitan adquirir evidencia sin modificar innecesariamente los medios originales; durante cada procedimiento de adquisición que lo requiera. Evidencia: registro del dispositivo utilizado, configuración, herramienta forense y bitácora de adquisición.
- Preservar dispositivos y medios de respaldo mediante mecanismos de almacenamiento controlado que eviten pérdida, modificación o acceso no autorizado a las copias de evidencia; durante todo el período de investigación y conservación de la evidencia. Evidencia: registros de almacenamiento, controles de acceso, inventario y bitácora de custodia.
- Proteger la evidencia frente a interferencias electromagnéticas, contaminación física o manipulación mediante elementos de protección adecuados, incluyendo protección electromagnética, guantes y materiales de aislamiento; durante la manipulación, transporte y almacenamiento de los elementos que lo requieran. Evidencia: registro de elementos utilizados, fotografías y lista de verificación de preservación.
- Utilizar medios de almacenamiento formateados o estériles mediante su preparación y verificación previa a la adquisición, evitando que contengan información residual que pueda contaminar la evidencia; antes de cada procedimiento de adquisición. Evidencia: registro de preparación, identificación del medio y resultado de verificación.

- Documentar visualmente la escena y los elementos recolectados mediante fotografías digitales que registren su ubicación, estado, conexiones, identificación y condiciones encontradas antes de su manipulación; antes, durante y después de la recolección cuando resulte necesario para preservar el contexto. Evidencia: fotografías originales, metadatos y referencia cruzada con el registro de evidencia.
- Embalar los elementos recolectados mediante cinta, bolsas para evidencia, bolsas antiestáticas, cajas, papel de burbuja, rótulos y demás materiales apropiados según el tipo de elemento, evitando daños físicos, contaminación o alteración; inmediatamente después de la recolección y antes del traslado o almacenamiento. Evidencia: fotografías del embalaje, etiquetas, registro de evidencia y cadena de custodia.

Condiciones previas al análisis forense

- Verificar y registrar que el evento haya sido previamente reportado mediante la consulta del sistema institucional de gestión de incidentes, confirmando su clasificación como incidente que afecta la confidencialidad, integridad o disponibilidad de información o datos personales; antes de iniciar la adquisición de evidencia digital. Evidencia: ticket de incidente, clasificación y registro de validación.
- Evaluar la necesidad de realizar análisis forense mediante criterios de impacto, naturaleza del incidente, requisitos legales o regulatorios, posibilidad de compromiso de información, necesidad de atribución y requerimientos de preservación de evidencia; antes de iniciar actividades forenses y cuando nuevas circunstancias modifiquen la valoración inicial. Evidencia: análisis de necesidad, decisión documentada y criterios aplicados.
- Confirmar la ocurrencia del incidente mediante la correlación de alertas, logs, evidencias técnicas, reportes y demás fuentes disponibles,

diferenciando entre eventos legítimos, falsos positivos e incidentes confirmados; antes de iniciar la adquisición formal de evidencia. Evidencia: análisis técnico, registros correlacionados y decisión documentada.

- Validar la necesidad de recolectar evidencia digital mediante la evaluación del tipo de incidente, activos afectados, información comprometida, volatilidad de los datos y posibilidad de pérdida o alteración; antes de realizar acciones sobre los sistemas involucrados. Evidencia: evaluación de evidencia requerida, alcance de adquisición y autorización correspondiente.

Identificación, recolección y preservación

- Minimizar la pérdida o alteración de información mediante técnicas de adquisición controlada, uso de bloqueadores de escritura cuando sean aplicables, trabajo sobre copias y restricción de modificaciones sobre los originales; durante todas las actividades de identificación, adquisición, traslado, almacenamiento y análisis. Evidencia: registros de adquisición, configuraciones de herramientas, hashes y bitácoras.
- Recolectar evidencia de medios volátiles mediante procedimientos que prioricen memoria RAM, conexiones de red, procesos activos, sesiones, conexiones abiertas y demás información susceptible de desaparecer, antes de apagar o reiniciar los equipos cuando las condiciones lo permitan; cuando la naturaleza del incidente y el estado del sistema indiquen que existe información volátil relevante. Evidencia: volcados de memoria, capturas de conexiones, procesos, comandos ejecutados y registros de adquisición.
- Capturar imágenes forenses de los medios digitales mediante herramientas especializadas que permitan realizar copias bit a bit y

conservar los datos originales sin modificación; durante cada adquisición de medios que requiera preservación forense. Evidencia: imagen forense, identificación del medio original, herramienta utilizada y registro de adquisición.

- Verificar la integridad de las copias mediante la generación y comparación de valores hash u otros mecanismos de validación apropiados entre el medio original y la copia adquirida; inmediatamente después de cada adquisición y antes de utilizar la copia para análisis. Evidencia: valores hash, informe de verificación y registro de integridad.
- Registrar todas las actividades realizadas sobre la evidencia mediante una bitácora cronológica que incluya fecha, hora, acción ejecutada, herramienta utilizada, evidencia involucrada, resultado y observaciones; durante todo el ciclo de adquisición, análisis, transferencia, almacenamiento y disposición de la evidencia. Evidencia: bitácora de actuaciones, logs de herramientas y registros de actividad.
- Analizar la totalidad de los datos recolectados mediante técnicas apropiadas al tipo de evidencia, correlacionando fuentes y preservando la trazabilidad de los hallazgos; durante la investigación y antes de emitir las conclusiones finales. Evidencia: resultados del análisis, consultas, filtros, líneas de tiempo y hallazgos.
- Documentar los hallazgos mediante un reporte técnico que relacione evidencia, hechos, análisis, conclusiones, limitaciones y recomendaciones, diferenciando hechos comprobados de hipótesis o inferencias; al finalizar el análisis y antes del cierre de la investigación. Evidencia: informe de hallazgos, anexos técnicos y evidencias referenciadas.

Cadena de custodia

- Inventariar y describir los elementos recolectados mediante un registro único que incluya número de evidencia, tipo de elemento, fabricante/modelo cuando aplique, número de serie, estado físico, ubicación, características relevantes y descripción detallada; inmediatamente después de la identificación y antes del embalaje. Evidencia: formato de inventario, fotografías y registro de evidencia.
- Embalar y sellar cada elemento mediante un contenedor adecuado a sus características físicas y técnicas, utilizando materiales que eviten manipulación, contaminación, daño o acceso no autorizado, y aplicando un sello o mecanismo de cierre verificable; inmediatamente después de su recolección y antes de cualquier traslado. Evidencia: evidencia fotográfica, identificación del contenedor, sello y registro de embalaje.
- Etiquetar cada evidencia mediante una identificación única que incluya fecha y hora del hallazgo, número de evidencia, número de registro o folio, ubicación exacta, descripción del material y observaciones relevantes; al momento de su recolección y antes de su almacenamiento o traslado. Evidencia: etiqueta, fotografías y formato de registro de evidencia.
- Registrar las personas que intervienen en la recolección y embalaje mediante nombre completo, identificación cuando corresponda, actividad realizada, fecha y hora de intervención; en el momento de cada actuación sobre la evidencia. Evidencia: formato de cadena de custodia, bitácora y registros de entrega.
- Mantener la cadena de custodia mediante una hoja de ruta que registre identificación de la evidencia, descripción, fecha y hora de cada transferencia, ubicación, custodio, identificación de quien entrega y recibe, actividad realizada y firmas correspondientes; cada vez que la evidencia sea trasladada, entregada, recibida, almacenada, examinada

o devuelta. Evidencia: hoja de ruta, formatos de entrega y recepción, firmas y registros de almacenamiento.

- Verificar la integridad de la cadena de custodia mediante la comparación de los registros de entrega, recepción, sellos, identificadores, ubicación y estado físico de la evidencia, antes de cada transferencia y durante las revisiones previas al análisis o cierre del caso. Evidencia: lista de verificación, registros de custodia, fotografías y actas de entrega/recepción.

8.8.2. Continuidad de la seguridad de la información

Control Asociado en el MSPI A.5.30

Incluir en el plan de continuidad del negocio y el plan de recuperación ante desastres criterios de seguridad de la información.
Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Participar y validar los requisitos de seguridad y privacidad mediante la revisión de los escenarios de contingencia, controles de acceso, protección de información, comunicaciones seguras, respaldo, recuperación y demás medidas aplicables durante las pruebas de los planes de recuperación ante desastres; en cada ejercicio de recuperación y antes de su cierre, verificando que los controles definidos sean aplicables durante la contingencia. Evidencia: plan y guion de prueba, listas de verificación, resultados de validación, hallazgos y actas de prueba.
- Identificar y valorar los riesgos de seguridad y privacidad asociados con la disponibilidad de los activos críticos mediante el análisis de su criticidad, dependencias tecnológicas, RTO, RPO, amenazas, vulnerabilidades y consecuencias de indisponibilidad, utilizando los

resultados del BIA y la metodología institucional de gestión de riesgos; durante la actualización del análisis de continuidad y ante cambios relevantes en procesos, sistemas o activos críticos. Evidencia: BIA, matriz de riesgos, inventario de activos críticos y plan de tratamiento.

La SIDT

- Aplicar medidas de continuidad y recuperación mediante redundancia, respaldos, infraestructura alterna, procedimientos de contingencia, mecanismos de comunicación y recuperación priorizada de servicios, de acuerdo con los niveles de criticidad y RTO/RPO definidos; durante situaciones de emergencia y mediante pruebas periódicas de efectividad. Evidencia: estrategias de continuidad, configuraciones, registros de respaldo, procedimientos de recuperación y resultados de pruebas.
- Activar y ejecutar el plan de recuperación definido en el LINEAMIENTO PLAN DE PRUEBAS DE RECUPERACION, ante desastres mediante procedimientos de escalamiento, declaración de contingencia, priorización de servicios, recuperación de infraestructura, aplicaciones y datos, y validación funcional posterior, cuando se presente una situación que cumpla los criterios de activación y durante los ejercicios programados. Evidencia: registros de activación, bitácoras de recuperación, tiempos obtenidos, resultados de validación y actas de cierre.
- Identificar y tratar los hallazgos derivados de pruebas, revisiones y monitoreos mediante un plan de acciones que registre hallazgo, riesgo asociado, medida de tratamiento, prioridad, fecha de inicio, fecha objetivo, estado y seguimiento, posterior a cada prueba o revisión y hasta verificar el cierre de las acciones. Evidencia: plan de tratamiento, tickets, registros de seguimiento, resultados de pruebas y evidencias de

cierre.

- Determinar y priorizar las aplicaciones y componentes de software de mayor impacto mediante un BIA que valore criticidad del proceso, impacto por indisponibilidad, dependencias, usuarios afectados, RTO, RPO y requisitos de recuperación; actualizar la valoración periódicamente y ante cambios significativos en procesos, aplicaciones o arquitectura tecnológica. Evidencia: BIA, matriz de criticidad, inventario de aplicaciones y resultados de actualización.
- Implementar estrategias de continuidad para aplicaciones y sistemas mediante mecanismos diferenciados según su criticidad, tales como redundancia, alta disponibilidad, respaldos, recuperación en infraestructura alterna, procedimientos manuales o soluciones de contingencia, de acuerdo con los resultados del BIA y los RTO/RPO establecidos. Evidencia: estrategias documentadas, arquitectura de continuidad, configuraciones, procedimientos y resultados de pruebas.
- Actualizar y controlar la documentación del plan de recuperación ante desastres mediante revisión de escenarios, servicios críticos, dependencias, contactos, procedimientos, recursos, RTO/RPO y estrategias de recuperación, como mínimo una vez al año y después de cambios tecnológicos, organizacionales, pruebas o incidentes relevantes. Evidencia: versión vigente del plan, control de cambios, actas de revisión y registros de aprobación.
- Capacitar y sensibilizar al personal mediante sesiones teóricas, ejercicios prácticos y simulaciones sobre activación del plan, funciones durante la contingencia, comunicación, recuperación y medidas de seguridad y privacidad, de acuerdo con el plan de capacitación y después de cambios relevantes en los procedimientos de recuperación. Evidencia: plan de capacitación, material utilizado, registros de asistencia, evaluaciones y

resultados de ejercicios.

- Incorporar controles de seguridad y privacidad en los procedimientos de recuperación mediante la identificación de controles aplicables durante la contingencia, tales como autenticación, control de acceso, cifrado, monitoreo, protección de respaldos y segregación de ambientes; durante la elaboración, actualización y prueba de cada estrategia de recuperación. Evidencia: procedimientos de recuperación, matrices de controles, configuraciones y listas de verificación.
- Implementar controles compensatorios mediante medidas alternativas previamente definidas cuando un control tecnológico no pueda operar durante una contingencia, considerando controles manuales, restricciones temporales de acceso, supervisión reforzada, monitoreo adicional o segregación de funciones; durante la activación de la contingencia y hasta la restauración del control original. Evidencia: registro del control afectado, análisis de riesgo, autorización, medida compensatoria, bitácoras y validación de retorno al control normal.
- Ejecutar pruebas de activación del plan de recuperación definidas en el LINEAMIENTO PLAN DE PRUEBAS DE RECUPERACION ante desastres mediante escenarios controlados que permitan verificar procedimientos de declaración, escalamiento, comunicación, recuperación, seguridad, continuidad y retorno a la operación, siguiendo el Lineamiento Plan de Pruebas de Recuperación; con la periodicidad establecida en el programa de pruebas y después de cambios significativos. Evidencia: plan y guion de prueba, resultados, tiempos de recuperación, hallazgos, evidencias técnicas y acta de cierre.
- Ejecutar pruebas de restauración de software y hardware definidas en el LINEAMIENTO PROGRAMA FORMAL DE PRUEBAS DE RESTAURACION, mediante la recuperación controlada de copias de respaldo, imágenes,

configuraciones, aplicaciones, bases de datos y componentes tecnológicos, siguiendo el Lineamiento Programa Formal de Pruebas de Restauración; conforme al cronograma establecido y después de cambios relevantes en los mecanismos de respaldo o recuperación. Evidencia: registros de restauración, respaldos utilizados, tiempos obtenidos, validaciones funcionales, resultados RTO/RPO y reporte de prueba.

- Verificar la efectividad de las restauraciones mediante pruebas de integridad, disponibilidad, funcionamiento y consistencia de la información recuperada, comparando los resultados con los criterios de aceptación definidos; al finalizar cada prueba de restauración y antes de declarar recuperado el servicio. Evidencia: resultados de validación, registros de integridad, pruebas funcionales, evidencias de disponibilidad y actas de aceptación.
- Definir y aplicar controles compensatorios para los controles tecnológicos que no puedan implementarse durante una crisis mediante una evaluación rápida del riesgo, identificación del control afectado, determinación de la medida alternativa, establecimiento de vigencia y definición de criterios de retorno al control normal; desde la identificación de la indisponibilidad del control hasta su restablecimiento y verificación. Evidencia: evaluación de riesgo, registro del control compensatorio, autorización, bitácoras de aplicación y evidencia de restablecimiento.

8.8.3. Gestión de capacidad

Control Asociado en el MSPI A.8.6

Garantizar capacidad necesaria de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones. Por lo tanto, se desarrollarán las siguientes actividades:

- Monitorear y proyectar el consumo de capacidad de procesamiento, memoria, almacenamiento, red y demás recursos tecnológicos mediante herramientas de monitoreo y análisis de tendencias, considerando el comportamiento histórico, crecimiento esperado, criticidad de los servicios y demanda proyectada; realizar la revisión con una periodicidad definida y ante incrementos significativos de demanda. Evidencia: reportes de capacidad, tendencias de consumo, proyecciones, alertas y registros de ampliación o provisión de recursos.
- Optimizar el uso de los servicios tecnológicos y sistemas de información mediante el análisis de utilización, rendimiento, disponibilidad y tiempos de respuesta, aplicando ajustes de configuración, distribución de cargas, liberación de recursos o ampliaciones cuando se identifiquen desviaciones respecto de los niveles esperados; efectuar la verificación periódicamente y ante degradaciones del servicio. Evidencia: informes de desempeño, registros de configuración, métricas de utilización, tickets de optimización y resultados de las verificaciones.
- Verificar periódicamente la capacidad de los servicios de red mediante el seguimiento del ancho de banda, utilización de enlaces, latencia, disponibilidad, saturación y crecimiento del tráfico, generando alertas cuando se superen los umbrales establecidos y aplicando acciones de ajuste o ampliación cuando corresponda. Evidencia: reportes de monitoreo de red, gráficas de utilización, alertas, análisis de tendencias, configuraciones y registros de acciones correctivas.
- Monitorear y revisar el uso y desempeño de la infraestructura tecnológica mediante indicadores de CPU, memoria, almacenamiento, red, disponibilidad, tiempos de respuesta y utilización de recursos,

comparando los resultados con los umbrales definidos y generando acciones de soporte cuando se presenten desviaciones; realizar el seguimiento de forma continua y consolidar los resultados periódicamente. Evidencia: tableros de monitoreo, informes de capacidad, alertas, tickets de soporte y registros de seguimiento.

- Implementar un plan de gestión de capacidad para los sistemas críticos mediante la identificación de recursos requeridos, niveles actuales de utilización, umbrales, proyecciones de crecimiento, riesgos de saturación y acciones de ampliación u optimización, revisándolo periódicamente y ante cambios significativos en los sistemas o en la demanda. Evidencia: plan de capacidad, matriz de sistemas críticos, análisis de demanda, proyecciones, cronograma de acciones y registros de seguimiento.
- Evaluar la utilización de capacidades de computación en la nube mediante el análisis de demanda, criticidad, elasticidad requerida, costos, disponibilidad, seguridad, protección de la información y capacidad de crecimiento, antes de incorporar o ampliar servicios tecnológicos que puedan beneficiarse de dicha modalidad. Evidencia: análisis técnico, evaluación de alternativas, estudio de capacidad, concepto de viabilidad y decisión documentada.
- Analizar la necesidad de reducir la demanda de nuevos recursos tecnológicos mediante la identificación de consumos innecesarios, recursos subutilizados, duplicidad de servicios, aplicaciones obsoletas y oportunidades de optimización, aplicando acciones de depuración, consolidación, automatización o racionalización antes de solicitar ampliaciones de capacidad. Evidencia: análisis de utilización, inventarios, reportes de recursos subutilizados, acciones de optimización y registros de liberación o consolidación.

Gestión Administrativa

- Proyectar y gestionar la capacidad de los recursos físicos mediante el análisis de ocupación, utilización de espacios, crecimiento de personal, necesidades operativas y proyecciones de expansión, revisando periódicamente la disponibilidad y determinando oportunamente la necesidad de nuevos espacios o adecuaciones. Evidencia: estudios de capacidad física, inventarios de espacios, proyecciones de crecimiento, informes de ocupación y solicitudes de adecuación o ampliación.
- Monitorear y verificar la capacidad de la infraestructura física mediante inspecciones, registros de ocupación, revisión de condiciones de las instalaciones y seguimiento de requerimientos de espacio, identificando oportunamente situaciones de sobreocupación, insuficiencia o deterioro que puedan afectar la operación; realizar las verificaciones periódicamente y ante cambios relevantes en las necesidades institucionales. Evidencia: informes de inspección, registros de ocupación, reportes de mantenimiento, solicitudes de adecuación y acciones de mejora.

Talento Humano

- Proyectar y gestionar la capacidad de los recursos humanos mediante el análisis de cargas de trabajo, estructura organizacional, funciones, niveles de servicio, disponibilidad de personal y proyecciones de crecimiento, realizando revisiones periódicas dentro de la gestión del desempeño y ante cambios significativos en las actividades institucionales. Evidencia: análisis de cargas laborales, proyecciones de personal, informes de desempeño, matrices de necesidades y planes de gestión del talento.

- Evaluar la necesidad de incorporación de nuevo personal mediante la comparación entre la capacidad disponible, las cargas de trabajo, las funciones requeridas, las brechas identificadas y las metas institucionales, documentando la justificación y priorización de las necesidades antes de iniciar los procesos de vinculación. Evidencia: análisis de brechas, estudios de carga laboral, solicitudes de personal, justificaciones y registros de aprobación.

8.8.4. Respaldo de información

Control Asociado en el MSPI A.8.13

Respaldar la información, software e imágenes de los sistemas de la ANCP-CCE, por medio de copias de seguridad, siguiendo los lineamientos establecidos en el documento LINEAMIENTO DE COPIAS DE RESPALDO Y RESTAURACIÓN ANCP Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

Gestión de copias de respaldo y restauración

- Implementar y mantener el esquema institucional de copias de respaldo mediante un procedimiento formal que establezca alcance, tipos de información, periodicidades, retención, ubicaciones, protección, restauración, recuperación ante desastres y pruebas, aplicándolo a la infraestructura tecnológica y actualizándolo ante cambios relevantes o resultados de pruebas. Evidencia: procedimiento aprobado, matriz de respaldos, registros de actualización y resultados de revisión.
- Clasificar y seleccionar la información, software, configuraciones e imágenes de sistemas que requieren respaldo mediante el inventario de activos, clasificación de la información, criticidad y requisitos de continuidad, revisando esta cobertura periódicamente y ante la

incorporación, modificación o retiro de activos. Evidencia: inventario de activos, matriz de información respaldada y registro de cobertura.

- Aplicar las estrategias de respaldo completa, incremental y diferencial mediante la configuración de las herramientas de backup de acuerdo con la criticidad, volumen, RPO y necesidades de recuperación de cada activo, verificando periódicamente que las tareas programadas correspondan a la estrategia definida. Evidencia: matriz de estrategia de respaldo, configuraciones, programación de tareas y reportes de ejecución.
- Verificar el funcionamiento integral del esquema de respaldo y custodia mediante la revisión de ejecuciones, disponibilidad de las copias, integridad, capacidad de almacenamiento, accesibilidad y controles de protección, realizando verificaciones periódicas y después de cambios relevantes en la infraestructura. Evidencia: reportes de backup, registros de integridad, alertas, bitácoras de custodia y resultados de verificaciones.
- Establecer y revisar los períodos de retención y frecuencia de las copias mediante el análisis de RPO, continuidad operativa, necesidades de consulta histórica, clasificación y criticidad de la información, validándolos previamente con los requerimientos del activo y revisándolos ante cambios en el negocio o en los sistemas. Evidencia: matriz de retención y frecuencia, análisis de RPO, registros de validación y aprobaciones.
- Documentar y actualizar los elementos tecnológicos y operativos que intervienen en cada etapa del respaldo y restauración mediante matrices de infraestructura, procedimientos, diagramas de flujo y registros de configuración, manteniendo la información actualizada ante modificaciones en la plataforma. Evidencia: matriz de componentes,

diagramas, procedimientos y registros de cambios.

- Controlar la ubicación de las copias mediante la definición de repositorios, centros de datos, almacenamiento local y ubicaciones externas, considerando volumen, capacidad, clasificación, retención y requisitos de continuidad; verificar periódicamente la disponibilidad y capacidad de cada ubicación. Evidencia: inventario de repositorios, matriz de ubicaciones, reportes de capacidad y registros de disponibilidad.
- Ejecutar y validar el proceso de recuperación mediante procedimientos documentados que contemplen selección del punto de restauración, recuperación de datos/configuraciones, validación de integridad y comprobación funcional, aplicándolo cuando ocurra una pérdida de información o durante las pruebas programadas. Evidencia: solicitudes de restauración, bitácoras, registros de recuperación, resultados de integridad y validación funcional.
- Programar y controlar la ejecución de las copias mediante la plataforma institucional de backup, configurando calendarios, dependencias, alertas y condiciones de ejecución, revisando los resultados de cada tarea y gestionando oportunamente los fallos detectados. Evidencia: programación de tareas, reportes de ejecución, alertas, tickets de fallos y registros de corrección.
- Proteger las copias de respaldo mediante cifrado, controles de acceso, segregación de privilegios, protección contra modificación o eliminación no autorizada y mecanismos de integridad, aplicando controles de acuerdo con la clasificación y los riesgos identificados para la información respaldada. Evidencia: configuraciones de cifrado, políticas de acceso, registros de permisos, logs y resultados de verificaciones de seguridad.
- Implementar y administrar una plataforma de copias de respaldo con

capacidad de automatización, monitoreo, generación de reportes, escalabilidad y recuperación, incorporando los recursos tecnológicos requeridos para atender el crecimiento de la infraestructura y las necesidades de continuidad. Evidencia: arquitectura de la solución, inventario de componentes, configuraciones, licenciamiento y reportes de operación.

Cobertura mínima de los respaldos

- Configurar y verificar el respaldo de servidores de archivos mediante políticas que incluyan las carpetas institucionales identificadas en el inventario de información, ejecutando las tareas según la periodicidad definida y validando sus resultados. Evidencia: políticas de backup, inventario de carpetas, reportes y pruebas de restauración.
- Respaldar servidores que soporten aplicaciones web y aplicaciones locales mediante políticas diferenciadas de acuerdo con su criticidad, RPO y dependencia de los servicios, verificando periódicamente la recuperación de los componentes respaldados. Evidencia: matriz de aplicaciones, políticas de respaldo, reportes y pruebas de recuperación.
- Respaldar información, aplicaciones y datos almacenados en servidores mediante la selección de archivos, volúmenes, configuraciones, imágenes o componentes requeridos para su recuperación, validando periódicamente que la copia permita reconstruir el servicio. Evidencia: políticas de respaldo, inventario, reportes de ejecución y pruebas de restauración.
- Respaldar bases de datos mediante mecanismos compatibles con cada plataforma, considerando consistencia, integridad, frecuencia, retención y RPO, ejecutando controles de validación y pruebas de recuperación periódicas. Evidencia: configuraciones de backup, logs de bases de

datos, reportes y resultados de restauración.

- Respaldar controladores de dominio, DHCP y configuraciones de elementos de red mediante la exportación o copia controlada de configuraciones y estados necesarios para su recuperación, ejecutándola después de cambios significativos y conforme a la periodicidad establecida. Evidencia: archivos de configuración, registros de backup, bitácoras de cambios y pruebas de recuperación.
- Respaldar las configuraciones de switches, routers y dispositivos de seguridad mediante mecanismos de exportación segura y almacenamiento protegido, ejecutando copias después de cambios relevantes y realizando verificaciones periódicas de disponibilidad e integridad. Evidencia: archivos de configuración, registros de ejecución, inventario y pruebas de recuperación.
- Evaluar la necesidad de respaldar estaciones de trabajo mediante el análisis de criticidad de la información local, dependencia operativa y posibilidad de recuperación desde fuentes institucionales, aplicando el respaldo cuando el análisis determine que su pérdida genera un impacto significativo. Evidencia: análisis de criticidad, matriz de cobertura, autorización y configuración de respaldo.

Almacenamiento y custodia

- Definir y dimensionar el almacenamiento on-site y off-site mediante el cálculo de volumen actual, crecimiento proyectado, frecuencia, retención, RPO y capacidad disponible, revisando las necesidades periódicamente y ante cambios significativos en la infraestructura. Evidencia: estudio de capacidad, proyecciones, matriz de almacenamiento y reportes de utilización.
- Implementar al menos dos copias de la información mediante

repositorios independientes, manteniendo como mínimo una copia fuera de las instalaciones cuando las condiciones técnicas y contractuales lo permitan, y aplicando mecanismos de segregación, integridad e inmutabilidad que reduzcan el riesgo de replicar corrupción, cifrado malicioso o eliminación. Evidencia: inventario de copias, arquitectura de respaldo, configuración de repositorios, reportes de integridad y pruebas de recuperación.

- Aplicar controles de seguridad física y lógica equivalentes o acordes al nivel de riesgo en los sitios principal, alterno y demás ubicaciones de procesamiento mediante controles de acceso, protección ambiental, vigilancia, segregación, autenticación y monitoreo, verificándolos durante las evaluaciones periódicas de infraestructura. Evidencia: controles de acceso, registros de ingreso, inspecciones, configuraciones, informes de seguridad y resultados de evaluación.
- Implementar y mantener un sitio alterno para almacenamiento de copias mediante la clasificación de la información y priorización de los activos según criticidad, RTO/RPO y necesidades de recuperación, verificando periódicamente su disponibilidad y capacidad. Evidencia: matriz de priorización, inventario del sitio alterno, reportes de capacidad y pruebas de recuperación.
- Identificar y rotular cada copia de respaldo mediante un esquema que registre activo, sistema, fecha, hora, tipo de copia, período de retención, ubicación y estado de integridad, aplicándolo durante la generación, traslado y custodia de cada copia. Evidencia: etiquetas, metadatos, inventario de copias y registros de custodia.

Monitoreo, pruebas y restauración

- Monitorear las ejecuciones de respaldo mediante una plataforma

centralizada que genere reportes y alertas sobre tareas exitosas, fallidas, incompletas, eliminaciones, modificaciones o indisponibilidad de repositorios, realizando seguimiento a las fallas hasta su corrección. Evidencia: tableros, reportes, alertas, tickets y registros de solución.

- Ejecutar y documentar pruebas de restauración de archivos, bases de datos, configuraciones, aplicaciones e imágenes como mínimo una vez cada semestre, seleccionando muestras representativas de acuerdo con criticidad y RPO/RTO, y verificando integridad, disponibilidad y funcionamiento de la información recuperada. Evidencia: plan de pruebas, guiones, bitácoras, tiempos de recuperación, resultados, evidencias técnicas y actas de cierre.
- Verificar durante cada prueba de restauración que los procedimientos, accesos, herramientas y mecanismos definidos permitan recuperar efectivamente la información, registrando las desviaciones y generando acciones correctivas cuando los resultados no cumplan los criterios establecidos. Evidencia: listas de verificación, resultados de pruebas, hallazgos, planes de acción y pruebas de cierre.
- Ejecutar pruebas de funcionamiento y capacidad del hardware y software utilizado para respaldos mediante pruebas de almacenamiento, lectura/escritura, recuperación, conectividad, integridad y operación de las herramientas, realizándolas como mínimo una vez al año y ante la incorporación de nueva infraestructura. Evidencia: plan y resultados de pruebas, registros técnicos, informes de capacidad y documentación de la infraestructura evaluada.
- Analizar y actualizar periódicamente el RPO de los sistemas de información mediante la revisión de criticidad, impacto por pérdida de datos, frecuencia de transacciones, necesidades operativas y resultados de las pruebas de recuperación, ajustando la estrategia de respaldo

cuando se identifiquen nuevas necesidades. Evidencia: BIA/análisis de impacto, matriz RPO, análisis de necesidades y configuración actualizada.

- Verificar periódicamente que las copias disponibles permitan recuperar las versiones requeridas mediante la selección de puntos de restauración, comprobación de integridad y ejecución de restauraciones controladas, priorizando los sistemas críticos y las copias más recientes. Evidencia: reportes de integridad, pruebas de restauración y registros de validación.

Frecuencias mínimas de respaldo

- Ejecutar respaldos diferenciales semanales de servidores de bases de datos, servidores web, sistemas de información, aplicaciones y dispositivos de red y seguridad, conforme a la matriz de respaldo y RPO definidos. Evidencia: programación, logs de ejecución y reportes semanales.
- Ejecutar respaldos completos mensuales de servidores de bases de datos, servidores web, sistemas de información, aplicaciones y dispositivos de red y seguridad, verificando la disponibilidad e integridad de las copias generadas. Evidencia: logs, reportes de backup, inventario de copias y verificaciones de integridad.
- Ejecutar respaldos completos anuales de los componentes tecnológicos definidos en la estrategia institucional, verificando que las copias sean recuperables y manteniéndolas durante el período de retención establecido. Evidencia: reportes de ejecución, inventario de copias, registros de retención y pruebas de recuperación.
- Ejecutar respaldos adicionales cada vez que se produzcan cambios significativos en sistemas operativos, configuraciones básicas, bases de

datos, aplicaciones, infraestructura o dispositivos críticos, verificando posteriormente la disponibilidad de la copia. Evidencia: solicitud o registro de cambio, backup asociado, logs y validación posterior.

Administración de la infraestructura de respaldo

- Actualizar las configuraciones de servidores y plataformas de respaldo mediante la aplicación controlada de parámetros, agentes, políticas y rutas requeridas para la correcta ejecución de las copias, realizando la revisión periódicamente y después de cambios en la infraestructura. Evidencia: configuraciones, registros de cambio, reportes de validación y logs de backup.
- Mantener la infraestructura necesaria para generar, almacenar y restaurar copias mediante repositorios, librerías, unidades de almacenamiento, conectividad, herramientas de backup y mecanismos de recuperación dimensionados según volumen, criticidad, RPO, RTO y crecimiento proyectado. Evidencia: inventario de infraestructura, diagramas, estudios de capacidad, configuraciones y pruebas de recuperación.
- Aplicar controles de integridad a las copias mediante mecanismos de verificación, hashes, validación de consistencia, pruebas de lectura/restauración y, cuando sea técnicamente viable, almacenamiento inmutable o protegido contra modificación, verificándolos de forma periódica. Evidencia: resultados de integridad, hashes, logs, configuraciones de inmutabilidad y pruebas de restauración.
- Capacitar y validar las competencias técnicas requeridas para la ejecución de respaldos y restauraciones mediante sesiones prácticas, procedimientos documentados y ejercicios controlados, realizando

actualización de conocimientos ante cambios relevantes en las plataformas. Evidencia: plan de capacitación, material, registros de asistencia, evaluaciones y resultados de ejercicios.

Reporte de eventos e incidentes

- Reportar y registrar los eventos o incidentes relacionados con pérdida, daño, robo, corrupción, indisponibilidad o compromiso de activos de información asociados a copias de respaldo o procesos de restauración mediante los canales institucionales de gestión de incidentes, incluyendo fecha, activo afectado, descripción, impacto, acciones ejecutadas y evidencias disponibles, inmediatamente después de su identificación y hasta su cierre. Evidencia: ticket o registro del incidente, alertas, logs, evidencias técnicas, comunicaciones, análisis y reporte de cierre.

8.8.5. Redundancia de instalaciones de tratamiento de información

Control Asociado en el MSPI: 8.14

Garantizar el funcionamiento continuo de instalaciones de procesamiento de información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Asesorar los proyectos que se desarrollen en la entidad mediante la revisión de sus diseños, arquitecturas, requerimientos y planes de continuidad, durante las etapas de formulación, diseño y aprobación, verificando la incorporación de componentes de resiliencia digital orientados a mantener la disponibilidad de los servicios de TI. Evidencia: conceptos, listas de verificación, actas de revisión y documentos técnicos de los proyectos.

La SIDT

- Reportar a Seguridad de la Información los eventos e incidentes que puedan generar pérdida, daño, robo o compromiso de activos de información mediante los canales y procedimientos establecidos para la gestión de incidentes, de manera inmediata o dentro de los tiempos definidos según la criticidad del evento, incluyendo la información necesaria para su análisis y tratamiento. Evidencia: registros de incidentes, tickets, reportes y comunicaciones de notificación.
- Gestionar la disponibilidad de las redes y servicios críticos mediante la contratación y mantenimiento de dos o más proveedores independientes, cuando el análisis de riesgos y los requerimientos de continuidad así lo determinen, priorizando servicios críticos como conectividad a Internet y comunicaciones. Evidencia: contratos, acuerdos de niveles de servicio (SLA), órdenes de servicio y registros de disponibilidad.
- Implementar redundancia geográfica para los servicios e instalaciones críticas de procesamiento mediante el uso de dos centros de datos ubicados a una distancia mínima de 20 km lineales, o mediante servicios en la nube que dispongan de infraestructura y sistemas duplicados, de acuerdo con los resultados del análisis de riesgos y los requerimientos de disponibilidad. Evidencia: arquitectura tecnológica, contratos de servicios, diagramas de infraestructura y análisis de riesgos.
- Implementar redundancia de los componentes tecnológicos críticos mediante la duplicación de elementos cuya falla pueda afectar la disponibilidad, tales como CPU, fuentes de alimentación, discos, memorias, cortafuegos, enrutadores y conmutadores, de acuerdo con la criticidad del servicio y los requerimientos de disponibilidad establecidos.

Evidencia: inventarios de infraestructura, diagramas de arquitectura, configuraciones y registros de mantenimiento.

- Implementar redundancia de los componentes de software mediante la ejecución de múltiples instancias de las aplicaciones y servicios críticos, utilizando mecanismos automáticos de distribución y balanceo de carga, cuando los requerimientos de disponibilidad y capacidad del servicio lo establezcan. Evidencia: configuraciones de balanceadores, arquitecturas de solución, registros de operación y pruebas de disponibilidad.
- Planificar y ejecutar pruebas de conmutación y activación de los componentes redundantes y de las instalaciones alternas de procesamiento mediante escenarios controlados de falla y recuperación, con la periodicidad definida en los planes de continuidad y recuperación, verificando los tiempos de recuperación y el funcionamiento de los servicios. Evidencia: planes y cronogramas de pruebas, resultados, registros de ejecución, informes y planes de mejora.
- Implementar mecanismos de monitoreo y alerta sobre fallas en las instalaciones y componentes de procesamiento de información mediante herramientas de supervisión de infraestructura, aplicaciones, comunicaciones y servicios, de forma continua, generando notificaciones ante condiciones que puedan afectar la disponibilidad. Evidencia: alertas, registros de monitoreo, dashboards, tickets e informes de disponibilidad.
- Evaluar e implementar tecnologías y servicios en la nube que permitan establecer redundancia de los recursos tecnológicos mediante arquitecturas de alta disponibilidad, replicación, distribución geográfica o mecanismos equivalentes, cuando el análisis de riesgos, los requerimientos de continuidad y disponibilidad lo justifiquen. Evidencia: evaluaciones técnicas, arquitecturas de nube, configuraciones, contratos

y resultados de pruebas.

- Establecer y aplicar lineamientos para la operación del SOC (Security Operations Center) mediante la definición de capacidades, procesos, mecanismos de monitoreo, correlación de eventos, gestión de alertas, escalamiento y respuesta ante incidentes de seguridad, de acuerdo con el modelo operativo y los niveles de servicio establecidos, verificando periódicamente su funcionamiento y cobertura. Evidencia: lineamientos del SOC, procedimientos, matrices de escalamiento, reportes de monitoreo, indicadores e informes de operación.

8.9. Componente Política de legal y Cumplimiento

8.9.1. Cumplimiento de requisitos legales, estatutarios y contractuales

Control Asociado en el MSPI: 5.32

Evitar incumplimientos mediante la identificación y cumplimiento de requisitos legales y regulatorios aplicables. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Jurídica

- Mantener actualizado el catálogo normativo o normograma mediante la identificación, análisis, registro y clasificación de los requisitos legales, regulatorios y normativos nacionales e internacionales aplicables a la seguridad y privacidad de la información, revisándolo como mínimo una vez al año y cada vez que se presenten cambios normativos relevantes. Evidencia: normograma vigente, registros de actualización, matrices de requisitos y fuentes normativas consultadas.
- Verificar y aplicar los requisitos legales, reglamentarios, regulatorios e internos relacionados con seguridad y privacidad de la información mediante su incorporación en políticas, procedimientos, controles y

demás instrumentos del SGSI, de acuerdo con la normativa aplicable y cada vez que se identifiquen nuevos requisitos o cambios regulatorios. Evidencia: matrices de cumplimiento, políticas y procedimientos actualizados, conceptos jurídicos y registros de verificación.

- Establecer la frecuencia de revisión y validación de los requisitos legales mediante criterios basados en la criticidad, nivel de cambio normativo, impacto sobre la información y obligaciones aplicables, definiendo como mínimo una revisión anual y revisiones extraordinarias ante cambios regulatorios. Evidencia: cronograma de revisión, metodología, matriz de requisitos y registros de seguimiento.
- Revisar periódicamente la legislación y reglamentación aplicable mediante el seguimiento de fuentes oficiales, boletines normativos, comunicaciones de organismos reguladores y mecanismos de actualización jurídica, como mínimo con periodicidad anual y ante la publicación de nuevas disposiciones o modificaciones relevantes. Evidencia: registros de monitoreo normativo, boletines, reportes de revisión y análisis de cambios.
- Actualizar el catálogo normativo mediante la incorporación, modificación o eliminación de requisitos derivados de cambios en la legislación, regulación o normatividad interna, cada vez que se identifique una modificación o nuevo requisito aplicable y como resultado de la revisión periódica. Evidencia: historial de versiones, registro de cambios y normograma actualizado.

Seguridad de la Información

- Verificar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con seguridad y privacidad de la información mediante la aplicación de listas de verificación,

matrices de cumplimiento, revisión documental y evaluación de controles, de acuerdo con el cronograma establecido y ante cambios significativos en los requisitos aplicables. Evidencia: informes de cumplimiento, matrices de evaluación, listas de verificación, hallazgos y planes de tratamiento.

- Dirección de Gestión de Innovación y Tecnología
- Documentar y actualizar los requisitos estatutarios, regulatorios y contractuales aplicables a cada sistema de información mediante la identificación de las obligaciones asociadas al servicio, información tratada, arquitectura, contratos y normativa aplicable, como mínimo una vez al año y cada vez que se implementen cambios relevantes o se generen nuevos requerimientos. Evidencia: matriz de requisitos por sistema, fichas técnicas, registros de actualización, contratos y documentos de control de cambios.

Funcionarios y terceros de la entidad

- Aplicar las obligaciones legales, estatutarias, reglamentarias y contractuales relacionadas con seguridad y privacidad de la información mediante el cumplimiento de las políticas, procedimientos, controles, acuerdos y demás disposiciones vigentes, durante el desarrollo de sus actividades y mientras mantengan acceso a información o recursos de la entidad. Evidencia: registros de aceptación de políticas, acuerdos de confidencialidad, evidencias de capacitación, registros de acceso y resultados de verificaciones de cumplimiento.

8.10. Componente Política de Revisión Independiente

8.10.1. Revisión independiente de la seguridad de la información

Control Asociado en el MSPI: 5.35

Validar la eficacia de los controles de seguridad mediante revisiones independientes. Por lo tanto, se desarrollarán las siguientes actividades:

Oficina de Control Interno y/o quien haga sus veces

- Revisar el cumplimiento de la implementación del Modelo de Seguridad y Privacidad de la Información mediante auditorías independientes que incluyan la evaluación de objetivos de control, políticas, procesos, procedimientos y controles de seguridad de la información, de acuerdo con el programa de auditoría establecido, a intervalos planificados y cuando se presenten cambios significativos. Las revisiones deben ser ejecutadas por personal con las competencias requeridas y coordinadas previamente con las dependencias involucradas. Evidencia: programa y plan de auditoría, listas de verificación, papeles de trabajo, informes y registros de hallazgos.
- Comunicar los resultados de las revisiones y auditorías mediante informes formales dirigidos a las dependencias evaluadas, una vez finalizada cada auditoría o revisión, documentando los hallazgos, incumplimientos, riesgos y oportunidades de mejora identificados. Evidencia: informes de auditoría, comunicaciones de resultados y registros de socialización.
- Almacenar los resultados de las revisiones y auditorías en repositorios institucionales con controles de acceso, integridad y trazabilidad, inmediatamente después de su aprobación y durante el periodo de conservación establecido, garantizando el acceso autorizado de las

dependencias involucradas y de Seguridad de la Información. Evidencia: repositorio definido, registros de acceso, control de versiones y matriz de permisos.

- Verificar la implementación y eficacia de las acciones correctivas mediante el seguimiento de los planes de acción, revisión de evidencias y validación del cierre de los hallazgos, en las fechas de seguimiento establecidas y hasta confirmar la eliminación o mitigación de la causa identificada. Evidencia: matrices de seguimiento, evidencias de implementación, resultados de las verificaciones y registros de cierre.
- Informar a la Alta Dirección sobre el avance en la implementación del Modelo de Seguridad y Privacidad de la Información mediante informes periódicos que consoliden el estado de cumplimiento, resultados de auditorías, hallazgos, riesgos, acciones correctivas e indicadores, de acuerdo con la periodicidad establecida para el seguimiento del modelo. Evidencia: informes de gestión, presentaciones, actas de comité y registros de seguimiento.
- Evaluar las oportunidades de mejora identificadas durante las revisiones de seguridad de la información mediante el análisis de sus causas, impacto, viabilidad y contribución al fortalecimiento del modelo, durante cada ciclo de auditoría, revisión o evaluación del SGSI/MSPI. Evidencia: matriz de oportunidades de mejora, informes de auditoría, análisis y planes de mejora.
- Analizar la necesidad de modificar el enfoque de seguridad de la información mediante la evaluación de resultados de auditorías, cambios organizacionales, tecnológicos, regulatorios, riesgos y amenazas emergentes, cuando se presenten cambios significativos o durante las revisiones periódicas del modelo. Evidencia: análisis de cambios, evaluaciones de riesgo, informes de auditoría, actas y propuestas de

actualización.

Jefes de las dependencias

- Formular planes de acción para corregir las deficiencias identificadas mediante el análisis de los hallazgos y la definición de actividades, responsables, recursos, fechas de ejecución, criterios de cumplimiento y mecanismos de seguimiento, dentro de los plazos establecidos para el tratamiento de cada hallazgo. Evidencia: plan de acción aprobado, matriz de seguimiento y cronograma de actividades.
- Registrar y reportar el avance de los planes de acción mediante la actualización periódica de la herramienta o carpeta institucional definida para el seguimiento por Seguridad de la Información, incorporando las evidencias que demuestren la ejecución y cierre de las actividades, con la periodicidad establecida y hasta el cierre de cada hallazgo. Evidencia: registros actualizados, soportes de ejecución, informes de avance y evidencias de cierre.

8.11. Componente Política de Seguridad Recursos Humanos

8.11.1. Comprobación de antecedentes de todos los candidatos

Control Asociado en el MSPI: 6.1

Verificar los antecedentes del talento humano de acuerdo con las leyes, los reglamentos, la ética y comprobar que cumpla con los requisitos de idoneidad, compromiso y responsabilidad inherentes al manejo de los activos de información a los que va a tener acceso y a los riesgos de seguridad y privacidad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

Talento Humano

- Verificar los antecedentes de funcionarios y contratistas mediante consultas en las fuentes oficiales y mecanismos de validación autorizados, como parte del proceso de selección y antes de formalizar la vinculación, de acuerdo con los requisitos legales y el perfil del cargo o servicio. Evidencia: resultados de consultas, formatos de verificación, listas de chequeo y soportes de selección.
- Validar la formación académica y experiencia profesional de funcionarios y contratistas mediante la revisión de títulos, certificaciones, referencias laborales y demás soportes aportados, durante el proceso de selección y antes de formalizar la vinculación. Evidencia: certificados, constancias de validación, registros de consulta y documentos de selección.
- Verificar la identidad de funcionarios y contratistas mediante la validación del documento de identidad o pasaporte expedido por la autoridad competente, antes de formalizar la vinculación y cuando se requiera actualizar la información de identificación. Evidencia: copia o registro autorizado del documento de identidad y constancia de validación.
- Revalidar los antecedentes de los funcionarios mediante la aplicación de los controles establecidos para selección, cuando se produzca un cambio de cargo que implique nuevas funciones, responsabilidades, privilegios o niveles de acceso a información y recursos. Evidencia: resultados de las verificaciones, registros de cambio de cargo y soportes de validación.

Compras y Contratos

- Verificar los antecedentes del personal vinculado mediante contratos de prestación de servicios utilizando una lista de verificación que contemple los requisitos legales, documentales y de seguridad aplicables, antes de la formalización del contrato y durante las renovaciones cuando

corresponda. Evidencia: lista de verificación diligenciada, consultas de antecedentes y documentos de soporte.

- Proteger la confidencialidad y reserva de la información contenida en las historias laborales mediante controles de acceso, clasificación de la información, almacenamiento seguro, gestión de permisos y trazabilidad de consultas o modificaciones, durante todo el ciclo de vida de los documentos y mientras exista obligación de conservación. Evidencia: matriz de permisos, registros de acceso, controles de seguridad, acuerdos de confidencialidad y registros de gestión documental.
- Ejecutar la vinculación y retiro de contratistas mediante la aplicación de los procedimientos internos, listas de verificación y controles documentales establecidos, antes de iniciar la prestación del servicio y al finalizar o terminar el vínculo contractual. Evidencia: listas de chequeo, documentos de vinculación y retiro, actas, paz y salvos y registros de cierre.

8.11.2. Términos y condiciones de trabajo

Control Asociado en el MSPI: 6.2

Asegurar de que el personal entiende sus responsabilidades en materia de seguridad de la información para las funciones para las que se considera. Por lo tanto, se desarrollarán las siguientes actividades:

Compras y Contratos

- Establecer los términos y condiciones de vinculación de terceros y funcionarios mediante cláusulas contractuales, anexos y acuerdos de confidencialidad que definan las obligaciones relacionadas con seguridad y privacidad de la información, propiedad intelectual, protección de datos personales, transparencia y acceso a la información pública, así como

las medidas aplicables ante incumplimientos, antes de formalizar la vinculación y durante las modificaciones o renovaciones contractuales. Evidencia: contratos, minutas, anexos, acuerdos de confidencialidad y registros de aprobación.

- Comunicar a los candidatos los términos y condiciones de vinculación mediante la entrega y explicación de las cláusulas contractuales y obligaciones de seguridad y privacidad de la información, indicando su aplicación durante y después de la relación con la entidad, antes de la formalización del vínculo contractual y señalando las consecuencias derivadas de su incumplimiento. Evidencia: constancias de entrega y aceptación, comunicaciones, contratos y documentos de vinculación.
- Formalizar los compromisos de confidencialidad de los funcionarios mediante la suscripción de acuerdos o cláusulas específicas que establezcan las obligaciones de protección, uso adecuado y reserva de la información, antes o durante la formalización de la vinculación y cuando se actualicen las condiciones aplicables. Evidencia: acuerdo de confidencialidad firmado e incorporado en la historia laboral.
- Incorporar en los contratos las consecuencias asociadas al incumplimiento de las políticas de seguridad de la información y al uso indebido o realización de acciones irregulares sobre los activos de información, mediante cláusulas que establezcan las medidas administrativas, contractuales y legales aplicables, antes de la formalización del contrato y en cada renovación o modificación que afecte dichas obligaciones. Evidencia: contratos, cláusulas de seguridad, anexos contractuales y registros de gestión de incumplimientos.

Talento Humano

- Formalizar las obligaciones de seguridad y privacidad de la información

aplicables a los funcionarios mediante acuerdos o cláusulas de confidencialidad que incorporen el cumplimiento de las políticas, lineamientos y directrices vigentes de la entidad, antes o durante la formalización de la vinculación y cuando se actualicen las condiciones de empleo. Evidencia: acuerdos de confidencialidad, documentos de vinculación y registros de aceptación.

- Establecer los términos y condiciones de empleo mediante documentos de vinculación que incorporen las obligaciones relacionadas con seguridad y privacidad de la información, propiedad intelectual, protección de datos personales, transparencia y acceso a la información pública, así como las consecuencias ante su incumplimiento, antes de formalizar la vinculación y cuando se modifiquen las condiciones aplicables. Evidencia: documentos de vinculación, acuerdos, reglamentos y registros de aceptación.
- Comunicar a los candidatos las condiciones y responsabilidades relacionadas con seguridad y privacidad de la información mediante la entrega y explicación de las obligaciones aplicables al cargo, incluyendo aquellas que permanezcan vigentes fuera de las instalaciones y del horario laboral, antes de formalizar la vinculación, informando las medidas aplicables ante su incumplimiento. Evidencia: constancias de entrega, registros de aceptación, documentos de vinculación y material de inducción.
- Formalizar los compromisos de confidencialidad de los contratistas mediante la suscripción de acuerdos o cláusulas específicas que establezcan las obligaciones de reserva, protección y uso adecuado de la información, antes o durante la formalización del contrato y cuando se modifiquen las condiciones que impliquen acceso a información. Evidencia: acuerdo de confidencialidad firmado e incorporado en el

expediente contractual.

8.11.3. Concientización, educación y capacitación en seguridad de la información

Control Asociado en el MSPI: 6.3

Garantizar que el personal, partes interesadas pertinentes conozcan y cumplan sus responsabilidades en materia de seguridad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Implementar un programa de concientización, educación y capacitación en seguridad y privacidad de la información mediante jornadas de sensibilización, capacitaciones, campañas, material educativo y ejercicios prácticos, con periodicidad definida y dirigido a funcionarios y terceros que tengan responsabilidades o acceso a activos de información, verificando la apropiación de los conocimientos y responsabilidades aplicables. Evidencia: programa aprobado, cronograma, contenidos, registros de asistencia, evaluaciones y reportes de participación.
- Desarrollar actividades de cultura, cambio y apropiación en seguridad y privacidad de la información mediante campañas, comunicaciones, talleres, simulaciones y actividades de sensibilización, de forma periódica y dirigidas a los usuarios internos con acceso a activos de información, considerando los riesgos y comportamientos identificados en la entidad. Evidencia: campañas realizadas, piezas de comunicación, registros de participación, resultados de ejercicios y métricas de apropiación.
- Ejecutar actividades periódicas de entrenamiento y actualización mediante capacitaciones, talleres, ejercicios prácticos y divulgación de

cambios en políticas, lineamientos y directrices, como mínimo una vez al año y adicionalmente cuando se presenten cambios normativos, tecnológicos, de riesgos o de políticas relevantes, reforzando la aplicación permanente de las responsabilidades de seguridad y privacidad asociadas a cada función. Evidencia: cronogramas, contenidos, registros de asistencia, evaluaciones de conocimiento y constancias de capacitación.

- Evaluar la ejecución y efectividad del programa de concientización, educación, capacitación y cultura mediante el seguimiento de indicadores de cobertura, participación, resultados de evaluaciones, comportamiento de los usuarios y cumplimiento de las actividades programadas, periódicamente y al cierre de cada ciclo de capacitación, identificando acciones de mejora cuando se presenten desviaciones. Evidencia: indicadores, informes de evaluación, resultados de encuestas y pruebas, análisis de brechas y planes de mejora.
- Definir y actualizar los contenidos generales de sensibilización mediante la identificación de riesgos comunes de seguridad y privacidad, requisitos legales y regulatorios, políticas, lineamientos, buenas prácticas, deberes, derechos, responsabilidades y consecuencias ante incumplimientos, incorporando pautas para el uso seguro de los activos de información, como mínimo anualmente y cuando se identifiquen nuevos riesgos, amenazas o cambios normativos. Evidencia: matriz de contenidos, material de sensibilización, presentaciones, campañas y registro de actualizaciones.
- Diseñar y mantener contenidos especializados de seguridad y privacidad mediante la identificación de los riesgos, controles y responsabilidades asociados a funciones específicas, incluyendo tecnología, desarrollo de software y tratamiento de datos personales, como mínimo anualmente

y cuando se incorporen nuevas tecnologías, procesos, sistemas o requisitos aplicables a estas actividades. Evidencia: programas de capacitación especializada, contenidos técnicos, material de entrenamiento, registros de asistencia y evaluaciones de conocimiento.

8.11.4. Proceso disciplinario

Control Asociado en el MSPI: 6.4

Garantizar que el personal y otras partes interesadas pertinentes entiendan las consecuencias de violación de política de seguridad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas pertinentes que cometieron violación. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Asesorar el traslado de los casos derivados de incidentes de seguridad y privacidad mediante la revisión de los reportes, resultados del análisis, evidencias, impacto y responsabilidades identificadas, cuando se determine la existencia de posibles conductas disciplinarias, administrativas o penales y de acuerdo con los procedimientos y requisitos legales aplicables. Evidencia: informes de incidentes, análisis de impacto, soportes de las evidencias, conceptos y registros de remisión a las instancias correspondientes.

Funcionarios y terceros

- Reportar comportamientos, eventos o situaciones que puedan constituir incumplimientos de las normas, políticas, procedimientos o lineamientos de seguridad y privacidad de la información mediante los canales institucionales establecidos para la gestión de incidentes y eventos de seguridad, de manera inmediata después de su identificación y

proporcionando la información y evidencias disponibles. Evidencia: reportes, tickets, registros de incidentes, comunicaciones y demás soportes asociados.

8.11.5. Responsabilidades después de la terminación o cambio de empleo

Control Asociado en el MSPI: 6.5

Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Establecer y habilitar mecanismos para el reporte de eventos o incidentes asociados con la pérdida, daño, robo o compromiso de activos de información derivados de la terminación o cambio de empleo, mediante canales institucionales de reporte y procedimientos de gestión de incidentes, cada vez que se produzca una desvinculación, traslado o modificación de las condiciones de vinculación. Evidencia: procedimiento de reporte, canales habilitados, registros de incidentes y tickets de atención.

Talento Humano

- Comunicar las obligaciones y deberes de seguridad y privacidad de la información que permanecen vigentes después de la terminación o cambio de empleo mediante la inclusión de cláusulas, acuerdos de confidencialidad, comunicaciones de retiro y demás mecanismos de notificación establecidos, durante el proceso de desvinculación o modificación de la vinculación. Evidencia: constancias de comunicación, acuerdos de confidencialidad, documentos de retiro y registros de

notificación.

- Solicitar la desactivación de los accesos tecnológicos mediante el registro de la novedad de retiro o cambio de empleo en la herramienta institucional de gestión de casos, incluyendo cuentas de usuario, VPN, credenciales y demás accesos que dejen de ser necesarios, antes o inmediatamente después de la fecha efectiva de terminación o modificación de la vinculación. Evidencia: solicitud o ticket de desactivación, registro de la novedad y confirmación de cierre de accesos.
- Notificar la terminación o modificación de la vinculación a la supervisión del servicio de vigilancia y seguridad privada mediante los canales institucionales establecidos, solicitando la desactivación de los mecanismos de control de acceso físico, en la fecha de terminación o modificación del vínculo y antes de que cese la necesidad de acceso a las instalaciones. Evidencia: comunicación de solicitud, registro de desactivación y reporte del sistema de control de acceso.
- Gestionar el diligenciamiento del Acta de Entrega mediante una lista de verificación que permita documentar la devolución de información, activos, recursos y accesos asociados a las funciones desempeñadas, como parte del proceso de desvinculación o cambio de empleo, exceptuando los casos de fallecimiento. Evidencia: Acta de Entrega diligenciada, lista de verificación y registros de validación.
- Recopilar y custodiar la información institucional mediante la identificación de los repositorios, dispositivos, medios y servicios utilizados durante la vinculación, realizando su entrega y almacenamiento en los repositorios institucionales autorizados, antes de la finalización efectiva del vínculo y de acuerdo con los tiempos de conservación aplicables. Evidencia: acta de entrega, inventarios de

información, registros de transferencia y constancias de custodia.

- Transferir la información institucional mediante mecanismos autorizados que garanticen su integridad, confidencialidad y trazabilidad, cuando por razones operativas o de continuidad sea necesario entregarla a otro funcionario, dependencia o repositorio institucional. Evidencia: registros de transferencia, actas de entrega, inventarios y confirmaciones de recepción.
- Verificar la devolución de los activos de información, la desactivación o eliminación de accesos físicos y lógicos y la transferencia de la información pertinente mediante una lista de chequeo de retiro y la validación de los registros correspondientes, antes del cierre definitivo del proceso de desvinculación o cambio de empleo. Evidencia: lista de verificación, acta de entrega, registros de devolución, confirmaciones de desactivación y evidencias de transferencia.

La SIDT

- Establecer y divulgar canales para la notificación de novedades de vinculación, traslado y desvinculación mediante la herramienta de gestión de casos, correo institucional u otros medios formalmente definidos, de manera permanente y cada vez que se produzca una modificación en la situación del personal. Evidencia: procedimiento publicado, comunicaciones, canales habilitados y registros de notificaciones recibidas.
- Desactivar o deshabilitar los accesos a los servicios tecnológicos mediante la gestión de las cuentas, perfiles, roles y permisos asociados al usuario, incluyendo dominio, cuentas administrativas y privilegiadas, VPN, escritorio virtual, sistemas de información, aplicativos legados y demás servicios, una vez recibida la solicitud formal de desvinculación o

modificación a través de la herramienta de gestión de casos y dentro del tiempo establecido para su atención. Evidencia: ticket de solicitud, registros de desactivación, bitácoras de sistemas y reporte de cierre de accesos.

- Generar y custodiar una copia de respaldo del buzón de correo electrónico mediante mecanismos de respaldo autorizados, una vez finalizada la vinculación y antes de eliminar o inhabilitar definitivamente la cuenta, manteniendo la copia en un ambiente controlado y sin habilitar el envío o recepción de mensajes desde el buzón respaldado. Evidencia: registro de respaldo, inventario de buzones, ubicación de la copia y bitácoras de acceso.
- Restringir la reutilización de las cuentas de correo electrónico asociadas a personal desvinculado mediante la inhabilitación permanente de sus credenciales y controles que impidan su reactivación para operación ordinaria, desde la terminación de la vinculación y durante el periodo de conservación del buzón, permitiendo únicamente su consulta o recuperación en ambientes offline cuando exista autorización y necesidad institucional. Evidencia: configuración de cuenta, registros de inhabilitación, bitácoras de acceso y evidencias del ambiente offline.
- Monitorear la gestión de roles y perfiles de acceso a la plataforma tecnológica mediante la revisión de registros de altas, modificaciones y bajas, correlacionándolos con las novedades de terminación contractual o desvinculación, de forma periódica y ante cada evento de retiro o cambio de vinculación, para detectar y corregir accesos que permanezcan habilitados sin justificación. Evidencia: reportes de monitoreo, bitácoras de acceso, matrices de roles y perfiles, tickets de ajuste y registros de revisión.

8.11.6. Acuerdos de confidencialidad o no divulgación

Control Asociado en el MSPI: 6.6

Proteger la información de la entidad y notificar a todos los usuarios internos, externos y proveedores de la ANCP-CCE sobre la responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada según lo especificado en el Manual para el tratamiento de datos personales y este manual. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Incorporar en los compromisos de confidencialidad y no divulgación cláusulas que regulen la duración de las obligaciones, su vigencia posterior a la terminación del vínculo, las condiciones de auditoría y monitoreo, el procedimiento de notificación de incidentes y las medidas aplicables ante incumplimientos, antes de su formalización y cada vez que se modifiquen las condiciones legales, contractuales o de tratamiento de la información. Evidencia: modelo de acuerdo vigente, control de versiones, conceptos jurídicos y registros de aprobación.
- Formalizar el compromiso de confidencialidad y no divulgación mediante un documento que incorpore las obligaciones de protección de la información, tratamiento de datos personales y demás requisitos establecidos, antes o durante la vinculación y cuando se modifiquen las condiciones de acceso o tratamiento de información. Evidencia: acuerdo firmado, autorización para tratamiento de datos personales y registro de vinculación.

Talento Humano

- Gestionar la suscripción del compromiso de confidencialidad y no divulgación mediante su incorporación en los documentos de vinculación

y la validación de su firma, antes de formalizar la vinculación del funcionario y como requisito para completar el proceso de ingreso. Evidencia: compromiso firmado, lista de verificación de vinculación y registro en la historia laboral.

- Verificar la existencia y validez del compromiso de confidencialidad y no divulgación mediante la revisión documental de su firma y fecha de suscripción, durante el proceso de vinculación y antes de habilitar las condiciones de acceso que correspondan. Evidencia: lista de chequeo, compromiso firmado y registro de validación.
- Revisar y actualizar los requisitos de los acuerdos de confidencialidad y no divulgación mediante el análisis de cambios normativos, contractuales, tecnológicos, riesgos de seguridad y condiciones de tratamiento de la información, como mínimo una vez al año y cada vez que ocurra un cambio que pueda afectar su contenido. Evidencia: acuerdo actualizado, matriz de cambios, registros de revisión y aprobación.

Compras y Contratos

- Formalizar la suscripción del compromiso de confidencialidad y no divulgación mediante su incorporación como requisito documental de los procesos contractuales y la validación de su firma, antes de iniciar la ejecución del contrato cuando exista acceso a información de la entidad. Evidencia: compromiso firmado, expediente contractual y lista de verificación de requisitos.
- Verificar la suscripción del compromiso de confidencialidad y no divulgación mediante la revisión del expediente contractual y la validación de la firma correspondiente, antes de autorizar el acceso del contratista a información o activos de la entidad. Evidencia: lista de

chequeo, compromiso firmado y registro de validación contractual.

- Incorporar en el manual y documentos de contratación el requisito de suscripción del compromiso de confidencialidad y no divulgación mediante cláusulas, listas de verificación y controles del proceso contractual, cuando el tercero requiera acceso a información de la ANCP-CCE y antes de iniciar dicho acceso. Evidencia: manual de contratación, minutas contractuales, listas de verificación y expedientes contractuales.
- Revisar y actualizar los requisitos de los acuerdos de confidencialidad y no divulgación mediante el análisis de cambios normativos, contractuales, tecnológicos, riesgos de seguridad y condiciones de acceso a la información, como mínimo una vez al año y cuando se presenten cambios que puedan afectar las obligaciones establecidas. Evidencia: acuerdos actualizados, registros de revisión, control de versiones y aprobaciones.

Supervisión de los contratos

- Solicitar y verificar la suscripción del compromiso de confidencialidad y no divulgación mediante la revisión del documento firmado y su incorporación al expediente contractual, antes de permitir el acceso del tercero a información de la ANCP-CCE y durante las modificaciones que impliquen nuevos accesos o información. Evidencia: solicitud, compromiso firmado, lista de verificación y expediente contractual.

Funcionarios y terceros

- Suscribir el compromiso de confidencialidad y no divulgación mediante la firma del documento establecido y la aceptación de las obligaciones de protección y uso adecuado de la información, antes de iniciar la

relación laboral, contractual o el acceso a información de la entidad. Evidencia: compromiso firmado y registro de vinculación.

- Revisar y comprender las obligaciones contenidas en el compromiso de confidencialidad y no divulgación mediante la lectura del documento, aclaración de inquietudes y aceptación expresa de sus condiciones, antes de su firma y cuando se produzcan modificaciones relevantes en las obligaciones. Evidencia: aceptación firmada, constancia de divulgación y registros de capacitación o sensibilización

8.12. Componente Política de Seguridad Física

8.12.1. Perímetros de seguridad física

Control Asociado en el MSPI:7.1

Impedir el acceso físico no autorizado, daños e interferencias en información de la organización y otros activos asociados. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Definir y delimitar los perímetros de seguridad física de las áreas tecnológicas que alberguen información e instalaciones de procesamiento sensibles o críticas mediante criterios de criticidad, análisis de riesgos y características de la infraestructura, implementando barreras físicas, cerraduras, alarmas y mecanismos de control de acceso, antes de habilitar las áreas y cada vez que se creen, modifiquen o trasladen instalaciones críticas. Evidencia: planos de áreas seguras, análisis de riesgos, inventarios de instalaciones, registros de controles implementados y documentación de infraestructura.
- Verificar la cobertura y funcionamiento de los sistemas de videovigilancia mediante inspecciones y revisión de las cámaras ubicadas en los

perímetros de seguridad, periódicamente y ante la implementación, modificación o falla de los sistemas de CCTV, asegurando la cobertura de los puntos de acceso y zonas críticas. Evidencia: registros de inspección, reportes de funcionamiento, grabaciones de prueba y registros de mantenimiento.

- Verificar el cierre y aseguramiento de puertas y ventanas de oficinas, salas e instalaciones que custodien activos de información de alta criticidad mediante inspecciones físicas y mecanismos de control de acceso, al finalizar la jornada laboral y durante los periodos en que las áreas permanezcan desocupadas, manteniendo vigilancia o supervisión permanente en espacios sin puertas cuando exista presencia de personal externo. Evidencia: listas de verificación, registros de inspección, bitácoras de vigilancia y reportes de novedades.
- Implementar y probar los sistemas de alarma asociados a las puertas contra incendios ubicadas en los perímetros de seguridad mediante mecanismos de detección, alerta y monitoreo, de acuerdo con el programa de mantenimiento y pruebas establecido y ante cualquier modificación o falla identificada. Evidencia: registros de pruebas, reportes de mantenimiento, bitácoras de alarmas y tickets de atención de fallas.
- Realizar análisis de riesgos y establecer planes de tratamiento para cada instalación o seccional mediante la identificación de amenazas, vulnerabilidades, activos críticos y controles existentes, como mínimo durante el ciclo periódico de gestión de riesgos y cuando se presenten cambios significativos en las instalaciones. Evidencia: matrices de riesgos, informes de análisis, planes de tratamiento y registros de seguimiento.
- Implementar y verificar los controles físicos de entrada a las

instalaciones y áreas seguras mediante mecanismos de identificación, autenticación, autorización, registro y monitoreo de accesos, de manera permanente y mediante revisiones periódicas de su funcionamiento, aplicando los criterios definidos por el Sistema de Gestión de Calidad y los lineamientos de seguridad física. Evidencia: procedimientos, registros de acceso, listas de autorizados, bitácoras, reportes de revisión y resultados de pruebas de control.

- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información derivados de fallas o vulneraciones de los perímetros de seguridad física mediante los canales institucionales establecidos para la gestión de incidentes, de manera inmediata después de su identificación, proporcionando la información y evidencias disponibles para su análisis y tratamiento. Evidencia: reportes, tickets, registros de incidentes, fotografías, grabaciones de CCTV y demás soportes disponibles.

Funcionarios y terceros

- Reportar los eventos e incidentes que involucren pérdida, daño, robo o compromiso de activos de información asociados con inconvenientes o vulneraciones de los perímetros de seguridad física mediante los canales institucionales establecidos, inmediatamente después de identificar el evento, suministrando la información y evidencias disponibles para facilitar su atención e investigación. Evidencia: reportes, tickets, comunicaciones, registros de incidentes y soportes del evento.

8.12.2. Acceso físico

Control Asociado en el MSPI: 7.2

Evitar accesos físicos no autorizados que atenten contra la confidencialidad, integridad o disponibilidad de la información de la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Implementar el control de acceso físico a las instalaciones, áreas seguras y zonas restringidas mediante mecanismos de identificación, autenticación, autorización y registro de ingreso, de forma permanente y de acuerdo con la clasificación de criticidad de cada área, restringiendo el acceso a personas previamente autorizadas. Evidencia: registros de acceso, listas de autorizados, credenciales y reportes de control.
- Proteger las zonas que contengan activos de información de alta criticidad mediante barreras físicas, cerraduras, alarmas, lectores de tarjetas, muros u otros mecanismos equivalentes, de acuerdo con los resultados del análisis de riesgos y la criticidad del área, verificando periódicamente su funcionamiento. Evidencia: inventario de controles físicos, registros de mantenimiento, pruebas de funcionamiento y reportes de inspección.
- Controlar el acceso a las áreas seguras mediante puntos de recepción con vigilancia, mecanismos electrónicos de control u otros medios equivalentes de identificación y autorización, en cada punto de acceso y durante todo el periodo de operación de las instalaciones. Evidencia: registros de ingreso, bitácoras de vigilancia, registros electrónicos y reportes de inspección.
- Registrar el ingreso de funcionarios, contratistas y visitantes mediante sistemas físicos o electrónicos de control de acceso, recopilando como

mínimo nombre, número de identificación, fecha y hora de ingreso y persona que autoriza el acceso, en cada ingreso a las instalaciones. Evidencia: registros de visitantes, bitácoras de recepción y reportes del sistema de control de acceso.

- Informar el tratamiento de los datos personales recopilados durante el control de acceso mediante avisos de privacidad ubicados en puntos visibles de ingreso y recepción, antes o al momento de la recolección de los datos y cada vez que se modifiquen las condiciones de tratamiento, conforme a la normativa aplicable. Evidencia: avisos de privacidad publicados, registros de actualización y material de divulgación.
- Asegurar las puertas de acceso a dependencias, oficinas, centros de cómputo, áreas de cableado y comunicaciones, salas de capacitación y demás zonas restringidas mediante cerraduras u otros mecanismos de control, durante las ausencias temporales del personal y cuando las áreas permanezcan desocupadas. Evidencia: inspecciones físicas, listas de verificación, registros de control de acceso y reportes de novedades.
- Verificar la efectividad de los controles físicos de entrada mediante inspecciones, pruebas de funcionamiento, revisión de registros y seguimiento de incidentes, de manera periódica y cuando se presenten cambios en las instalaciones, controles o niveles de riesgo. Evidencia: listas de verificación, informes de inspección, resultados de pruebas y planes de mejora.
- Delimitar las áreas de cargue, descargue y despacho mediante barreras físicas, señalización y controles de acceso que impidan la circulación no autorizada hacia otras áreas de las edificaciones, de manera permanente y cada vez que se modifique la distribución física. Evidencia: planos, señalización instalada, registros de inspección y controles de acceso.
- Vigilar las puertas externas de las áreas de cargue, descargue y

despacho mediante controles de vigilancia física o electrónica, durante todo el tiempo en que las puertas internas permanezcan abiertas, restringiendo el acceso de personas no autorizadas. Evidencia: bitácoras de vigilancia, registros de acceso y reportes de supervisión.

- Registrar los materiales que ingresan a las instalaciones mediante controles de recepción que permitan identificar el material, procedencia, fecha, hora, transportador y persona que recibe, en cada ingreso de materiales o mercancías. Evidencia: registros de recepción, formatos de ingreso, órdenes de compra y documentos de transporte.
- Inspeccionar los materiales que ingresan mediante revisión física y documental para identificar componentes peligrosos, daños, manipulación indebida o señales de alteración durante el transporte, en cada recepción y antes de permitir su ingreso a las áreas internas. Cuando se detecten anomalías, reportarlas inmediatamente mediante los canales de seguridad establecidos. Evidencia: registros de inspección, fotografías, actas de recepción, reportes de novedades y registros de incidentes.
- Identificar a las personas que ingresan a las instalaciones mediante el uso visible de carnés institucionales o credenciales autorizadas y, para el personal que acceda a zonas de cargue, descargue y despacho, mediante identificación de la empresa a la que pertenece y validación de los permisos correspondientes, durante todo el tiempo de permanencia en las instalaciones. Evidencia: registros de ingreso, credenciales, autorizaciones y bitácoras de vigilancia.
- Establecer y mantener controles físicos de acceso mediante procedimientos que definan mecanismos de autorización, identificación, registro, supervisión, revisión y atención de eventos, de manera permanente y mediante verificaciones periódicas de su funcionamiento.

Evidencia: procedimientos vigentes, registros de acceso, listas de verificación, informes de revisión y registros de incidentes.

Funcionarios y terceros

- Autorizar el ingreso temporal de visitantes mediante comunicación previa que registre la identidad del visitante, motivo, fecha, horario o duración de la visita y área autorizada, antes de permitir el ingreso a las instalaciones o áreas restringidas. Evidencia: comunicación de autorización, registro de visitantes y bitácora de ingreso.
- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información derivados de fallas en los controles físicos de entrada o salida, así como los ocurridos en áreas de despacho, cargue y descargue, mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación, aportando la información y evidencias disponibles. Evidencia: tickets, reportes de incidentes, comunicaciones, registros de vigilancia y grabaciones de CCTV.
- Gestionar los permisos de acceso a dependencias, oficinas, centros de cómputo, áreas de cableado y comunicaciones, salas de capacitación y demás zonas restringidas mediante autorización previa, asignación individual de permisos y controles físicos o electrónicos de ingreso, antes de conceder el acceso y durante todo el periodo en que se mantenga la necesidad de acceso, revisando y retirando los permisos cuando dejen de ser necesarios. Evidencia: matriz de permisos, solicitudes y autorizaciones, registros de acceso y reportes de revisión.

8.12.3. Aseguramiento de oficinas, salas e instalaciones

Control Asociado en el MSPI: 7.3

Impedir acceso físico no autorizado, daños e interferencias en información de la organización y otros activos asociados en ofi cinas, salas e instalaciones. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Implementar el sistema de detección de intrusos y alarmas físicas mediante sensores, dispositivos de alerta y mecanismos de activación configurados para detectar accesos no autorizados, manteniéndolo activo durante el horario laboral y conforme a las condiciones de seguridad definidas para las instalaciones. Evidencia: registros de configuración, bitácoras de activación y desactivación, reportes de eventos y pruebas de funcionamiento.
- Verificar el funcionamiento de los sistemas de detección de intrusos mediante pruebas controladas de activación, revisión de sensores, dispositivos de alerta y mecanismos de comunicación de eventos, de manera periódica y cada vez que se realicen modificaciones, mantenimientos o se presenten fallas. Evidencia: registros de pruebas, informes de mantenimiento, resultados de verificación y reportes de fallas o acciones correctivas.
- Registrar todos los ingresos y salidas de funcionarios, contratistas y visitantes mediante tarjeta de aproximación, sistema biométrico u otro mecanismo electrónico autorizado para la apertura de puertas, en cada ingreso o salida y sin excepciones, evitando el ingreso o salida de terceros mediante puertas previamente abiertas por otra persona. Evidencia: registros electrónicos de acceso, bitácoras de ingreso y salida y reportes de novedades.

- Controlar el cumplimiento del registro individual de acceso mediante supervisión de los puntos de entrada y salida, verificación de los registros electrónicos y reporte de situaciones en las que se permita el acceso sin utilizar el mecanismo autorizado, de manera permanente durante el horario de operación de las instalaciones. Evidencia: reportes de supervisión, registros de acceso, bitácoras de vigilancia y reportes de incumplimiento.
- Acompañar a los visitantes durante su permanencia en las dependencias donde se maneje información mediante asignación de un acompañante autorizado que supervise su desplazamiento y acceso a las áreas permitidas, durante todo el tiempo de permanencia en dichas áreas. Evidencia: registros de visitantes, autorizaciones de ingreso y bitácoras de acompañamiento.
- Presentar ante el personal de la dependencia correspondiente a los visitantes que requieran permanecer en las oficinas por más de dos días mediante comunicación previa de su identidad, motivo de permanencia y periodo autorizado, antes de iniciar la permanencia prolongada y cuando se produzcan cambios en las condiciones de acceso. Evidencia: registros de visitantes, comunicaciones de presentación y autorizaciones de permanencia.
- Establecer el horario autorizado para la recepción de visitantes mediante la definición y divulgación de franjas de atención y mecanismos de autorización excepcional, aplicándolo en cada ingreso y requiriendo autorización previa del nivel jerárquico correspondiente cuando el acceso se solicite fuera del horario establecido. Evidencia: horario publicado, registros de ingreso, autorizaciones excepcionales y bitácoras de recepción.
- Clasificar las instalaciones críticas mediante la evaluación de la criticidad

de los procesos, activos de información y actividades de procesamiento desarrolladas en cada área, como mínimo durante la revisión periódica de riesgos y cada vez que cambien los procesos, activos o condiciones de operación. Evidencia: matriz de criticidad, análisis de riesgos, inventario de áreas críticas y registros de actualización.

- Identificar las instalaciones críticas mediante mecanismos discretos de señalización y control que permitan su reconocimiento por el personal autorizado sin revelar públicamente su condición de criticidad, durante todo el periodo en que mantengan dicha clasificación y cada vez que esta sea modificada. Evidencia: registros de clasificación, planos controlados, inventario de áreas y verificaciones de seguridad física.
- Restringir el acceso a directorios, guías telefónicas internas y mapas mediante su ubicación en espacios físicos o repositorios de acceso controlado, utilizando cerraduras, permisos o mecanismos equivalentes, manteniéndolos fuera del alcance de visitantes y público en general y revisando periódicamente los permisos de acceso. Evidencia: registros de ubicación, controles de acceso, permisos autorizados y verificaciones de inspección.
- Analizar los riesgos de seguridad física de cada seccional mediante la identificación de amenazas, vulnerabilidades, impactos y controles existentes sobre oficinas, salas e instalaciones, como mínimo una vez al año y cada vez que se presenten cambios relevantes en infraestructura, operación o nivel de riesgo. Evidencia: matrices de riesgos, informes de análisis y registros de actualización.
- Tratar los riesgos identificados en las instalaciones mediante la formulación, priorización y seguimiento de acciones de mitigación de acuerdo con su nivel de riesgo y los lineamientos de seguridad física establecidos, dentro de los plazos definidos en el plan de tratamiento y

hasta verificar el cierre o aceptación formal del riesgo residual. Evidencia: planes de tratamiento, cronogramas, registros de seguimiento, evidencias de implementación y aceptación del riesgo residual.

- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información ocasionados por fallas en la seguridad de oficinas, recintos o instalaciones mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación, conservando la información y evidencias disponibles para su análisis. Evidencia: tickets, reportes de incidentes, comunicaciones, registros de vigilancia, fotografías, grabaciones de CCTV y demás soportes asociados.

8.12.4. Supervisión de seguridad física

Control Asociado en el MSPI: 7.4

Verificar periódicamente el acceso físico de funcionarios y terceros con acceso a la información de la organización y otros activos asociados en las oficinas, salas e instalaciones de la ANCP-CCE, para prevenir y detectar accesos no autorizados de forma oportuna a las instalaciones de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Instalar y operar sistemas de circuito cerrado de televisión (CCTV) mediante cámaras ubicadas estratégicamente para cubrir equipos, usuarios internos, visitantes y áreas donde se gestionen activos de información de alta criticidad, incluyendo zonas de cargue, descargue y despacho, de manera permanente y de acuerdo con la criticidad y los resultados del análisis de riesgos. Evidencia: inventario de cámaras, planos de cobertura, registros de configuración, grabaciones y reportes

de monitoreo.

- Informar el tratamiento de los datos personales capturados mediante CCTV y demás mecanismos de vigilancia física a través de avisos de privacidad visibles en los puntos de ingreso y áreas donde se realice la captación de imágenes, antes o al momento de la recolección y cada vez que se modifiquen las condiciones del tratamiento, conforme a la normativa aplicable. Evidencia: avisos de privacidad publicados, registros de actualización y soportes de verificación.
- Notificar y presentar a los funcionarios de la dependencia correspondiente a los visitantes que requieran permanecer de forma continua en las oficinas mediante comunicación previa de su identidad, motivo de permanencia y periodo autorizado, cuando la permanencia supere el número de días definido para cada dependencia y antes de iniciar dicho periodo. Evidencia: registros de visitantes, comunicaciones de notificación, autorizaciones y constancias de presentación.
- Verificar el funcionamiento de los detectores de contacto, sonido y movimiento mediante inspecciones físicas, pruebas controladas de activación y revisión de las señales generadas por los sistemas de alarma, de acuerdo con un cronograma previamente establecido, aprobado y actualizado, y adicionalmente cuando se presenten fallas, modificaciones o mantenimientos. Evidencia: cronograma vigente, registros de pruebas, informes de revisión, reportes de fallas y acciones correctivas.
- Activar los sistemas de alarma en las dependencias desocupadas mediante mecanismos de configuración automática o activación controlada, durante todo el periodo en que las áreas permanezcan sin ocupantes y especialmente cuando contengan equipos tecnológicos, de comunicaciones o activos de alta criticidad. Evidencia: registros de

activación y desactivación, bitácoras del sistema, reportes de eventos y registros de supervisión.

- Proteger los diseños, diagramas y documentación técnica de los sistemas de monitoreo mediante su clasificación como información "clasificada", almacenamiento en repositorios de acceso restringido y aplicación de controles de permisos y trazabilidad, durante todo su ciclo de vida y cada vez que sean consultados, modificados o actualizados. Evidencia: documentos clasificados, matriz de permisos, registros de acceso, historial de versiones y bitácoras de consulta.
- Proteger los paneles de control de los sistemas de alarmas mediante mecanismos físicos y lógicos que impidan o detecten su manipulación no autorizada, tales como cerraduras, sellos de seguridad, controles de acceso y registros de eventos, de manera permanente y mediante verificación periódica de su integridad. Evidencia: registros de inspección, controles de acceso, reportes de eventos, registros de mantenimiento y evidencias de integridad.
- Comprobar el funcionamiento de los sistemas de alarmas y monitoreo mediante pruebas controladas de sensores, paneles, comunicaciones, generación de alertas y mecanismos de respuesta, de acuerdo con la periodicidad definida por la entidad y cada vez que se realicen modificaciones, mantenimientos o se presenten incidentes o fallas. Evidencia: cronogramas de pruebas, resultados, bitácoras, informes técnicos, registros de alertas y acciones correctivas.
- Analizar los riesgos asociados a la supervisión de la seguridad física de cada seccional mediante la identificación de amenazas, vulnerabilidades, impactos y controles existentes en las instalaciones, como mínimo una vez al año y cada vez que se presenten cambios relevantes en infraestructura, operación, tecnología o nivel de riesgo. Evidencia:

matrices de riesgos, informes de análisis y registros de actualización.

- Implementar y hacer seguimiento a los planes de tratamiento de los riesgos identificados mediante acciones de mitigación, responsables de ejecución, fechas objetivo, recursos y criterios de cierre, de acuerdo con la prioridad del riesgo y hasta verificar la efectividad de las medidas implementadas. Evidencia: planes de tratamiento, cronogramas, registros de seguimiento, evidencias de implementación y resultados de verificación.

8.12.5. Protección contra amenazas físicas y medioambientales

Control Asociado en el MSPI: 7.5

Diseñar e implementar la protección contra amenazas físicas y ambientales, considerando desastres naturales, ataques maliciosos, accidentes y otras amenazas físicas intencionales o no intencionales a la infraestructura de la ANCP-CCE. Por lo tanto, se desarrollarán las siguientes actividades:

SIDT

- Alinear, revisar y actualizar los controles frente a amenazas externas y ambientales mediante la integración de medidas de prevención, protección, respuesta y recuperación en los planes de contingencia, emergencia, gestión del riesgo, evacuación y continuidad de la operación tecnológica, como mínimo una vez al año y cada vez que se presenten cambios en los riesgos, infraestructura, procesos o condiciones de operación. Evidencia: planes actualizados, matrices de controles, registros de revisión y versiones aprobadas.
- Monitorear las variables de temperatura y humedad de los centros de cómputo, áreas de cableado, comunicaciones y cuartos técnicos mediante sensores, sistemas de monitoreo y registros de medición, de

manera permanente y conforme a los rangos establecidos para cada ambiente y equipo. Evidencia: registros de temperatura y humedad, alertas del sistema, reportes de monitoreo y bitácoras de inspección.

- Reportar las desviaciones, daños o fallas de los sistemas de control ambiental mediante los canales institucionales de mantenimiento y gestión de novedades, inmediatamente después de su identificación y hasta verificar la normalización de las condiciones ambientales, solicitando el reemplazo, reparación o mantenimiento requerido. Evidencia: tickets de mantenimiento, reportes de novedades, órdenes de servicio, registros de intervención y resultados de verificación.
- Coordinar la elaboración y actualización del Plan de Continuidad y Recuperación de Desastres mediante la identificación de escenarios de interrupción, análisis de impactos, definición de estrategias de recuperación, RTO/RPO, recursos y procedimientos de respuesta, como mínimo una vez al año y ante cambios significativos en procesos, infraestructura, riesgos o servicios tecnológicos. Evidencia: Plan de Continuidad y Recuperación de Desastres, análisis de impacto, matriz de escenarios, estrategias y procedimientos de recuperación.
- Verificar la efectividad de los controles frente a amenazas externas y ambientales mediante ejercicios, simulaciones y pruebas de continuidad y recuperación, de acuerdo con el cronograma establecido y como mínimo una vez al año, documentando resultados, desviaciones y acciones de mejora. Evidencia: planes y registros de pruebas, resultados de simulaciones, informes de evaluación y planes de mejora.

Gestión Administrativa

- Establecer y mantener controles frente a amenazas externas y ambientales mediante su incorporación en los procedimientos

administrativos, protocolos de emergencia, mantenimiento e inspección de las instalaciones, de manera permanente y mediante revisión periódica de su aplicación y efectividad. Evidencia: procedimientos vigentes, listas de verificación, registros de inspección, reportes de mantenimiento y acciones de mejora.

- Implementar y verificar mecanismos de protección frente a temperatura, humedad, fuego y demás amenazas ambientales mediante sistemas y controles definidos de acuerdo con las especificaciones de los fabricantes de los equipos ubicados en centros de cómputo, áreas de cableado, comunicaciones y cuartos técnicos, de manera permanente y mediante inspecciones y mantenimientos periódicos. Evidencia: fichas técnicas, registros de instalación, mantenimiento, inspección y pruebas de funcionamiento.
- Monitorear las condiciones de temperatura y humedad de los cuartos de archivo mediante instrumentos de medición y registros periódicos, de acuerdo con los rangos ambientales definidos para la conservación documental y con seguimiento permanente o periódico según la criticidad del archivo. Evidencia: registros de medición, reportes de monitoreo, listas de inspección y alertas.
- Reportar y gestionar las desviaciones, daños o fallas que afecten las condiciones ambientales de los cuartos de archivo mediante los canales institucionales de mantenimiento, inmediatamente después de su identificación y hasta verificar la corrección de la condición detectada. Evidencia: reportes de mantenimiento, tickets, órdenes de servicio y registros de cierre.
- Identificar y valorar las amenazas externas que puedan afectar las instalaciones y los activos de información mediante análisis de riesgos, inspecciones de seguridad y revisión de escenarios de emergencia, como

mínimo una vez al año y cada vez que se presenten cambios relevantes en las instalaciones, entorno o nivel de riesgo. Evidencia: matrices de riesgos, informes de inspección y registros de actualización.

- Definir e implementar acciones preventivas y de mitigación frente a las amenazas identificadas mediante controles físicos, ambientales, administrativos y de respuesta, de acuerdo con el nivel de riesgo y dentro de los plazos establecidos en los planes de tratamiento. Evidencia: planes de tratamiento, registros de implementación, inspecciones y resultados de seguimiento.
- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información ocasionados por amenazas externas o ambientales mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación, conservando las evidencias disponibles para su análisis y tratamiento. Evidencia: tickets, reportes de incidentes, fotografías, registros de vigilancia, comunicaciones y demás soportes asociados.

Seguridad de la Información

- Alinear, revisar y actualizar los procesos de continuidad operativa y recuperación ante desastres relacionados con la infraestructura tecnológica mediante la incorporación de resultados del análisis de impacto, riesgos, dependencias tecnológicas, RTO/RPO y escenarios de interrupción, como mínimo una vez al año y cada vez que se presenten cambios significativos en la infraestructura, servicios o riesgos tecnológicos. Evidencia: planes actualizados, análisis de impacto, matrices de riesgos, procedimientos de recuperación y registros de revisión.

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Talento Humano

- Revisar y actualizar los documentos relacionados con la prevención y atención de emergencias mediante la validación de escenarios, niveles de emergencia, mecanismos de alarma, protocolos de actuación y medidas de seguridad física, como mínimo una vez al año y cada vez que se presenten cambios normativos, organizacionales o en los escenarios de emergencia. Evidencia: documentos actualizados, control de versiones, registros de revisión y listado maestro vigente.
- Aprobar y divulgar los documentos de prevención y atención de emergencias mediante los mecanismos institucionales de aprobación, publicación y comunicación, cada vez que se emita una nueva versión o se modifiquen los procedimientos aplicables. Evidencia: registros de aprobación, publicaciones, comunicaciones, material divulgado y constancias de socialización.
- Funcionarios y terceros de la entidad
- Aplicar los controles establecidos para la prevención y atención de emergencias mediante el seguimiento de los procedimientos, protocolos de evacuación, niveles de emergencia, mecanismos de alarma y demás instrucciones de seguridad física, durante la ocurrencia de eventos de emergencia, simulacros y ejercicios programados. Evidencia: registros de capacitación, asistencia a simulacros, evaluaciones, reportes de participación y registros de incidentes.

8.12.6. Trabajo en zonas seguras

Control Asociado en el MSPI:7.6

Proteger información y otros activos asociados en áreas seguras contra daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Gestionar los roles y permisos de acceso a las áreas seguras mediante una matriz de autorizaciones que relacione usuarios, áreas, niveles de acceso y vigencia de los permisos, antes de habilitar el acceso y cada vez que se produzcan cambios de funciones, traslados, desvinculaciones o modificaciones en las áreas. Evidencia: matriz de accesos, solicitudes y autorizaciones, registros de modificación y reportes de acceso.
- Revisar la asignación de privilegios de acceso a las áreas seguras mediante la comparación periódica entre los permisos asignados, las funciones vigentes y las necesidades de acceso, como mínimo de manera semestral y adicionalmente cuando se presenten cambios de personal o funciones. Evidencia: informes de revisión, matriz de permisos, registros de depuración y solicitudes de retiro o modificación de accesos.

Gestión Administrativa

- Implementar mecanismos de protección física, ambiental y de control de acceso mediante cerraduras, controles electrónicos, alarmas, sistemas de detección, condiciones ambientales y demás medidas definidas según la criticidad de cada área segura, de manera permanente y mediante verificaciones periódicas de su funcionamiento, restringiendo el ingreso exclusivamente a personas autorizadas. Evidencia: inventario de

controles, registros de acceso, inspecciones, mantenimientos y reportes de funcionamiento.

- Restringir y controlar el ingreso y permanencia de elementos inflamables dentro de las áreas seguras mediante prohibiciones, inspecciones físicas y mecanismos de almacenamiento controlado cuando su utilización sea necesaria, de manera permanente y durante cada inspección de seguridad. Evidencia: listas de verificación, registros de inspección, reportes de novedades y evidencias de almacenamiento.
- Señalizar las restricciones de seguridad en las áreas seguras mediante avisos visibles que indiquen la prohibición de fumar, comer y beber, manteniéndolos instalados de manera permanente y verificando su estado durante las inspecciones periódicas. Evidencia: registros fotográficos, listas de inspección y reportes de mantenimiento de señalización.
- Capacitar al personal encargado de la limpieza mediante instrucciones específicas sobre controles de acceso, manipulación de equipos, protección de activos, restricciones de ingreso y actuación ante incidentes, antes de iniciar actividades en áreas seguras y mediante refuerzos periódicos o cuando cambien las condiciones de seguridad. Evidencia: contenidos de capacitación, registros de asistencia, evaluaciones y constancias de socialización.
- Supervisar las actividades de limpieza en las áreas seguras mediante controles de ingreso, acompañamiento o verificación durante la ejecución de las labores y revisión de los elementos autorizados para ingresar, en cada jornada de limpieza, evitando el ingreso de maletas, bolsos u otros objetos ajenos a la actividad. Evidencia: registros de ingreso, listas de verificación, bitácoras de supervisión y reportes de novedades.

- Informar el tratamiento de datos personales realizado mediante los sistemas de videovigilancia a través de avisos de privacidad ubicados en puntos visibles de las áreas monitoreadas y de acceso a las instalaciones, antes o al momento de la captación de imágenes y cada vez que se modifiquen las condiciones del tratamiento. Evidencia: avisos publicados, registros de actualización y verificaciones de cumplimiento.
- Inspeccionar periódicamente las áreas seguras mediante listas de verificación que permitan validar el estado de puertas, cerraduras, controles de acceso, condiciones ambientales, señalización, restricciones y demás medidas de protección, de acuerdo con el cronograma establecido y cuando se presenten incidentes, cambios o condiciones anómalas. Evidencia: listas de verificación, informes de inspección, registros fotográficos y reportes de acciones correctivas.
- Verificar que las áreas seguras permanezcan vacías y aseguradas mediante inspecciones físicas y revisión de los controles de acceso, al finalizar las jornadas laborales, durante los periodos de inactividad y cuando las áreas no estén autorizadas para su ocupación. Evidencia: bitácoras de inspección, registros de acceso, reportes de vigilancia y listas de verificación.
- Restringir el uso de equipos fotográficos, de video, audio o grabación mediante controles de acceso, señalización y autorización previa para su utilización dentro de las áreas seguras, durante toda la permanencia en dichas áreas y cada vez que se requiera utilizar alguno de estos dispositivos. Evidencia: autorizaciones registradas, bitácoras de ingreso, reportes de inspección y registros de novedades.
- Monitorear las actividades desarrolladas en las áreas seguras mediante sistemas CCTV ubicados estratégicamente para cubrir accesos, circulación y actividades generales, de manera permanente,

configurando las cámaras de forma que no capturen directamente información sensible, pantallas o documentos en proceso de consulta. Evidencia: planos de ubicación de cámaras, configuración del sistema, registros de monitoreo, grabaciones y verificaciones de cobertura.

- Establecer y mantener los controles de seguridad de las áreas seguras mediante su incorporación en procedimientos, listas de verificación, protocolos de operación, inspección y mantenimiento, de manera permanente y mediante revisión periódica de su aplicación y efectividad, en concordancia con los lineamientos del Sistema de Gestión de Calidad. Evidencia: procedimientos vigentes, registros de revisión, listas de verificación, informes de inspección y acciones de mejora.
- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información ocurridos en áreas seguras mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación, conservando las evidencias disponibles para su análisis. Evidencia: tickets, reportes de incidentes, registros de acceso, grabaciones de CCTV, fotografías y comunicaciones.

SIDT

- Implementar mecanismos de protección física, ambiental y de control de acceso en los centros de datos mediante controles biométricos o electrónicos, cerraduras, alarmas, monitoreo ambiental y demás medidas definidas según la criticidad de la infraestructura tecnológica, de manera permanente y mediante verificaciones periódicas de funcionamiento, restringiendo el acceso exclusivamente al personal autorizado. Evidencia: registros de acceso, matriz de autorizaciones, inventario de controles, inspecciones y reportes de mantenimiento.

- Restringir y controlar el almacenamiento y permanencia de elementos inflamables en los centros de datos mediante prohibiciones, inspecciones físicas y mecanismos de almacenamiento seguro para aquellos elementos estrictamente necesarios para la operación, de manera permanente y durante las inspecciones periódicas de seguridad. Evidencia: listas de verificación, registros de inspección, reportes de novedades y evidencias de almacenamiento.
- Señalizar las restricciones de seguridad en los centros de datos mediante avisos visibles que indiquen la prohibición de fumar, comer y beber, manteniéndolos instalados de manera permanente y verificando periódicamente su estado y visibilidad. Evidencia: registros fotográficos, listas de inspección y reportes de mantenimiento.
- Supervisar las actividades de limpieza en los centros de datos mediante autorización previa, control de ingreso y acompañamiento durante la ejecución de las labores, verificando los elementos que ingresan a estas áreas, en cada jornada de limpieza, restringiendo el ingreso de maletas, bolsos u objetos que no sean necesarios para la actividad. Evidencia: registros de acceso, autorizaciones, bitácoras de supervisión y listas de verificación.
- Reportar los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos de información ocurridos en los centros de datos mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación, preservando los registros técnicos y evidencias disponibles. Evidencia: tickets, reportes de incidentes, registros de acceso, bitácoras, grabaciones de CCTV y soportes técnicos.
- Inspeccionar periódicamente los centros de datos mediante listas de verificación que permitan validar el estado de puertas, cerraduras,

controles de acceso, señalización, condiciones ambientales, restricciones y demás controles de seguridad, de acuerdo con el cronograma establecido y ante incidentes, cambios o condiciones anómalas. Evidencia: listas de verificación, informes de inspección, registros de acceso y reportes de acciones correctivas.

- Verificar que los centros de datos permanezcan vacíos y asegurados cuando no exista personal autorizado realizando actividades mediante revisión de los registros de acceso, inspección física y validación del estado de las cerraduras, al finalizar las jornadas de operación y durante los periodos en que no se requiera presencia de personal. Evidencia: bitácoras, registros electrónicos de acceso, listas de verificación y reportes de vigilancia.
- Restringir el ingreso y uso de equipos fotográficos, de video, audio o grabación mediante autorización previa y controles de acceso, durante toda la permanencia en los centros de datos y cada vez que se requiera utilizar estos dispositivos. Evidencia: autorizaciones, registros de ingreso, bitácoras y reportes de inspección.
- Monitorear las actividades desarrolladas en los centros de datos mediante sistemas CCTV orientados hacia accesos, zonas de circulación y áreas operativas, de manera permanente, evitando que las cámaras capturen directamente pantallas, documentos, credenciales u otra información sensible. Evidencia: planos de cobertura, configuración de cámaras, registros de monitoreo, grabaciones y verificaciones periódicas de la orientación de los dispositivos.

8.12.7. Escritorio y pantalla despejados

Control Asociado en el MSPI: 7.7

Reducir riesgos de acceso no autorizado, pérdida y daño de información en escritorios, pantallas y otros lugares accesibles durante y fuera del horario de trabajo. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Verificar y mantener los puestos de trabajo físicos y virtuales libres de documentos, carpetas, archivos y medios que contengan información sensible mediante inspecciones periódicas y aplicación de controles de escritorio y pantalla limpia, especialmente al finalizar la jornada y durante ausencias; evidencia: listas de verificación, registros de inspección, reportes de hallazgos y acciones correctivas.
- Capacitar y sensibilizar a instructores y asistentes sobre el cierre seguro de actividades en auditorios, salas de reuniones y salones de capacitación mediante instrucciones sobre recolección de materiales, eliminación segura de archivos, vaciado de papeleras digitales y borrado de información de tableros y carteleras, aplicándolas al finalizar cada actividad; evidencia: material de capacitación, registros de asistencia, listas de verificación y evidencias de cierre.
- Seguridad de la Información
- Sensibilizar y capacitar a funcionarios y terceros sobre el manejo seguro de documentos y archivos fuera de sus lugares de conservación mediante campañas, instrucciones y casos prácticos relacionados con clasificación de la información, custodia, acceso y divulgación, realizando las actividades durante la inducción y periódicamente; evidencia: plan y material de sensibilización, registros de asistencia, evaluaciones y comunicaciones realizadas.

- Aplicar controles de custodia de la información durante las ausencias temporales y al finalizar la jornada mediante el almacenamiento de documentos físicos en espacios cerrados y el cierre o bloqueo de los recursos electrónicos, de acuerdo con la clasificación de la información; evidencia: listas de verificación, inspecciones y registros de hallazgos.

Funcionarios y terceros de la entidad

- Bloquear las sesiones de computadores, portátiles, tabletas y teléfonos celulares mediante las funciones de bloqueo del sistema operativo o dispositivo cada vez que el usuario se ausente temporalmente de su puesto de trabajo; evidencia: configuración de bloqueo automático, registros de cumplimiento y verificaciones periódicas.
- Apagar los equipos de cómputo mediante los procedimientos establecidos cuando se presenten ausencias superiores a los tiempos definidos o al finalizar la jornada laboral, exceptuando los equipos que deban permanecer operativos para garantizar la continuidad de los servicios; evidencia: políticas de configuración, registros de apagado cuando estén disponibles y verificaciones de cumplimiento.
- Almacenar los archivos de trabajo en las carpetas institucionales habilitadas en OneDrive y SharePoint, evitando conservar información sensible, documentos o accesos directos en el escritorio local del equipo; realizar la verificación durante revisiones de seguridad o cuando se detecten riesgos de exposición. Evidencia: estructura de carpetas institucionales, configuraciones, reportes de almacenamiento y resultados de inspecciones.
- Resguardar los documentos físicos y electrónicos mediante archivadores, gavetas, repositorios institucionales, bloqueo de equipos y controles de acceso, aplicando las medidas al finalizar la jornada y cada vez que el

usuario se aleje del puesto de trabajo; evidencia: registros de inspección, listas de verificación y reportes de incumplimiento.

- Ubicar los computadores y portátiles de manera que las pantallas no sean visibles desde zonas de tránsito o por personas no autorizadas, complementando esta medida con filtros de privacidad cuando el nivel de sensibilidad o las condiciones del espacio lo requieran; evidencia: inspecciones físicas, listas de verificación y registros de medidas correctivas.
- Proteger las credenciales de autenticación mediante el uso de mecanismos institucionales de gestión de contraseñas y evitando registrarlas en papeles, equipos, escritorios o lugares accesibles a terceros; realizar verificaciones durante actividades de sensibilización e inspecciones de seguridad. Evidencia: material de sensibilización, resultados de inspecciones y reportes de hallazgos.
- Custodiar documentos, medios y dispositivos removibles autorizados mediante gavetas, archivadores o espacios bajo llave cuando no estén en uso y al finalizar la jornada, manteniendo restringido el acceso a personas no autorizadas; evidencia: registros de custodia, inspecciones y controles de inventario.
- Archivar los expedientes físicos mediante su traslado al archivo de gestión o espacio institucional autorizado al finalizar la jornada, aplicando las condiciones de organización, conservación y acceso establecidas para cada tipo de información; evidencia: registros de archivo, inventarios documentales y listas de verificación.
- Custodiar las llaves utilizadas para acceder a documentos o archivos físicos mediante su almacenamiento en lugares seguros y bajo control de acceso, evitando dejarlas sobre escritorios o en espacios visibles cuando no estén siendo utilizadas; evidencia: registros de entrega y

custodia de llaves, inspecciones y reportes de hallazgos.

- Destruir los documentos físicos que contengan información reservada o clasificada cuando haya finalizado su período de utilidad y no exista obligación de conservación, utilizando máquinas de destrucción o mecanismos seguros autorizados y depositando los residuos en los recipientes destinados para su disposición; evidencia: registros de destrucción, actas, controles de disposición y, cuando aplique, certificados de eliminación.
- Controlar la salida de información física, electrónica y activos de información de las instalaciones mediante autorización previa, registro de salida y validación de la necesidad de traslado, aplicando el control únicamente en los casos excepcionales autorizados; evidencia: solicitudes de autorización, registros de salida, inventarios y controles de préstamo o traslado.
- Prevenir la sustracción, destrucción, ocultamiento o utilización indebida de información mediante controles de acceso físico, custodia documental, bloqueo de equipos, almacenamiento seguro y aplicación de las reglas de escritorio y pantalla limpia, verificando su cumplimiento periódicamente; evidencia: inspecciones, listas de verificación, reportes de incidentes y acciones correctivas.
- Mantener los escritorios virtuales libres de documentos, carpetas, archivos y medios que contengan información sensible mediante el almacenamiento de la información en los repositorios institucionales autorizados y la eliminación periódica de archivos innecesarios, especialmente al finalizar la jornada o ante cambios de usuario/equipo; evidencia: inspecciones, reportes de almacenamiento y registros de depuración.

La SIDT

- Custodiar los dispositivos y medios removibles de almacenamiento mediante espacios físicos bajo llave, controles de acceso e inventarios actualizados, verificando periódicamente su ubicación, asignación y estado; evidencia: inventario de medios, registros de custodia, controles de préstamo e inspecciones.
- Configurar el bloqueo automático de computadores y portátiles mediante las políticas institucionales de seguridad y el protector de pantalla, estableciendo el tiempo máximo de inactividad definido para la entidad y verificando periódicamente su aplicación mediante herramientas de administración centralizada o inspecciones técnicas; evidencia: políticas de configuración, reportes de cumplimiento, configuraciones de equipos y resultados de pruebas.
- Configurar y verificar el apagado seguro de los equipos de cómputo para ausencias superiores a dos horas mediante políticas operativas y procedimientos de apagado. Evidencia: procedimientos, inventario de excepciones, configuraciones, registros de mantenimiento y verificaciones técnicas.
- Fortalecer y verificar los controles de escritorio y pantalla limpia mediante políticas de bloqueo automático, gestión de sesiones, controles de almacenamiento, protección de medios removibles, inspecciones físicas y campañas de sensibilización, revisando su efectividad periódicamente y ajustándolos cuando se identifiquen incumplimientos o nuevos riesgos; evidencia: políticas, configuraciones, informes de inspección, campañas, indicadores, hallazgos y planes de mejora.

8.12.8. Ubicación y protección de equipos

Control Asociado en el MSPI: 7.8

Ubicar y proteger los equipos para reducir los riesgos de amenazas, peligros del entorno y accesos no autorizados. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Ubicar los equipos y dispositivos que soportan funciones misionales y críticas en áreas con acceso restringido, mediante controles físicos de ingreso, cerraduras, registro de visitantes y supervisión de acceso, verificando periódicamente que su ubicación corresponda con la criticidad del activo. Evidencia: inventario de activos, matriz de ubicación y criticidad, registros de acceso e inspecciones físicas.
- Custodiar los dispositivos removibles y la información reservada o clasificada mediante almacenamiento en espacios cerrados y con acceso restringido durante horarios no hábiles o cuando los usuarios no se encuentren en sus puestos de trabajo. Evidencia: registros de custodia, controles de acceso, inspecciones y reportes de hallazgos.
- Ubicar equipos de cómputo, impresoras y demás dispositivos tecnológicos en espacios protegidos frente a acceso no autorizado, humedad, temperatura, polvo, vibraciones y otras condiciones ambientales que puedan afectar su funcionamiento, realizando inspecciones periódicas. Evidencia: inventario de ubicación, inspecciones físicas, reportes de mantenimiento y registros de condiciones ambientales.
- Implementar y mantener sistemas de protección eléctrica mediante UPS, reguladores, sistemas de puesta a tierra, protección contra sobretensiones y dispositivos contra descargas atmosféricas, verificando su funcionamiento mediante mantenimiento y pruebas periódicas y

después de eventos eléctricos relevantes. Evidencia: registros de mantenimiento, pruebas de UPS/protecciones, certificados técnicos e informes de inspección.

- Aplicar medidas de protección física y eléctrica sobre hardware, software y comunicaciones mediante controles de acceso, cerramientos, protección contra sobretensiones, sistemas de respaldo eléctrico, vigilancia y mecanismos de seguridad tecnológica, verificando periódicamente su efectividad frente a los riesgos identificados. Evidencia: matriz de controles, inspecciones, configuraciones, registros de mantenimiento y resultados de pruebas.
- Inspeccionar y monitorear periódicamente los dispositivos de seguridad instalados en centros de cómputo, cableado, comunicaciones y cuartos técnicos mediante pruebas funcionales, revisión de alarmas y mantenimiento preventivo, atendiendo oportunamente las fallas detectadas. Evidencia: listas de verificación, reportes de monitoreo, alarmas, órdenes de mantenimiento y registros de corrección.
- Proteger el cableado de energía y telecomunicaciones mediante canaletas, bandejas, ductos o sistemas equivalentes que eviten manipulación accidental, deterioro físico, interferencias y desconexiones, verificando su estado durante las inspecciones de infraestructura. Evidencia: planos de cableado, registros de inspección, fotografías técnicas y reportes de mantenimiento.
- Controlar el traslado o retiro de equipos entre dependencias o fuera de las instalaciones mediante autorización previa, identificación del activo, registro de salida y entrada, validación del custodio y actualización del inventario, aplicándolo en cada movimiento del activo. Evidencia: formatos de traslado, autorizaciones, registros de ingreso/salida e inventario actualizado.

- Restringir la exposición de activos de información reservada, clasificada o de datos personales no públicos mediante almacenamiento en repositorios autorizados, controles de acceso, eliminación de accesos directos innecesarios y aplicación de políticas de escritorio limpio, verificando periódicamente su cumplimiento. Evidencia: configuraciones, permisos, inspecciones, reportes de cumplimiento y registros de hallazgos.
- Formalizar y verificar los controles de ubicación y protección de equipos mediante su incorporación en procedimientos institucionales del Sistema de Gestión de Calidad, realizando revisiones cuando se presenten cambios tecnológicos, organizacionales o de riesgo. Evidencia: procedimientos aprobados, listas de verificación, registros de revisión y evidencias de aplicación.
- Reportar y registrar los eventos o incidentes relacionados con pérdida, daño, robo o compromiso de activos derivados de deficiencias en su ubicación o protección mediante los canales institucionales de gestión de incidentes, inmediatamente después de su identificación y hasta su cierre. Evidencia: tickets, reportes de incidentes, comunicaciones, evidencias técnicas y registros de cierre.
- Implementar mecanismos de protección y desconexión eléctrica de emergencia en centros de cómputo, cableado, comunicaciones y cuartos técnicos mediante interruptores, tableros, UPS y sistemas de protección compatibles con la infraestructura, verificando su funcionamiento durante mantenimientos y pruebas periódicas. Evidencia: diagramas eléctricos, certificados, pruebas, registros de mantenimiento y reportes de inspección.
- Mantener la infraestructura de procesamiento mediante contratos de mantenimiento y soporte que establezcan frecuencias, niveles de

servicio, atención de fallas, mantenimiento preventivo y correctivo, verificando su ejecución durante el período contractual. Evidencia: contratos, SLA, órdenes de servicio, informes de mantenimiento y actas de recibo.

Seguridad de la Información y seguridad tecnológica

- Proteger y monitorear la infraestructura de seguridad física y lógica mediante controles de acceso, monitoreo, mantenimiento preventivo y correctivo, revisión de configuraciones y actualización de componentes, ejecutando las actividades conforme a los ciclos definidos y ante eventos que puedan afectar su funcionamiento. Evidencia: registros de mantenimiento, configuraciones, logs, tickets e informes técnicos.
- Implementar y verificar dispositivos de detección temprana en centros de cómputo, cableado, comunicaciones y cuartos técnicos mediante sensores y sistemas de alarma para humo, temperatura, humedad, energía, acceso y otras condiciones críticas, realizando pruebas periódicas y atendiendo las alertas generadas. Evidencia: inventario de dispositivos, configuraciones, registros de alarmas, pruebas y mantenimientos.
- Aislar o restringir equipos cuando se detecte o sospeche infección por malware, virus o una falla física mediante desconexión de red, cuarentena, bloqueo de cuentas, suspensión de servicios o retiro controlado del equipo, aplicando el procedimiento de gestión de incidentes y realizando la validación antes de su reincorporación. Evidencia: alertas, tickets, registros de aislamiento, análisis técnico, resultados de remediación y autorización de reincorporación.
- Implementar y monitorear sistemas de detección y prevención de

incendios mediante sensores, alarmas, sistemas de extinción compatibles y mecanismos de notificación, realizando pruebas funcionales y mantenimiento periódico de acuerdo con las especificaciones técnicas. Evidencia: certificados, registros de mantenimiento, pruebas de alarma, reportes de inspección y registros de eventos.

- Autorizar y verificar el uso de equipos externos mediante una revisión previa de licenciamiento de software, actualización de antivirus, nivel de seguridad, configuración y cumplimiento de requisitos institucionales, realizando la validación antes de permitir su conexión o acceso a recursos institucionales. Evidencia: checklist de validación, autorización, inventario temporal y resultados de revisión técnica.
- Monitorear y notificar las alarmas relacionadas con suministro, regulación y estabilización eléctrica mediante los sistemas de monitoreo de UPS, reguladores y tableros eléctricos, generando alertas y escalamiento ante desviaciones que puedan afectar la infraestructura. Evidencia: logs eléctricos, alarmas, reportes de monitoreo, tickets y registros de atención.
- Aplicar controles de protección física y eléctrica en los centros de datos mediante control de acceso, vigilancia, protección contra sobretensiones, UPS, puesta a tierra, climatización, detección de incendios y mecanismos de continuidad, verificando su funcionamiento mediante inspecciones y pruebas periódicas. Evidencia: controles de acceso, registros ambientales, pruebas, mantenimientos y reportes de inspección.
- Reportar y gestionar los eventos o incidentes de seguridad asociados a centros de datos operados por terceros, ya sean on-premise, cloud o híbridos, mediante los canales institucionales y contractuales definidos,

registrando el evento, impacto, activos afectados y acciones ejecutadas desde su detección hasta el cierre. Evidencia: tickets, comunicaciones con proveedores, reportes técnicos, SLA, evidencias de atención y cierre.

- Ejecutar el mantenimiento preventivo y correctivo conforme a los intervalos, procedimientos y especificaciones del fabricante o proveedor, registrando las fallas identificadas, actividades realizadas, componentes intervenidos, fechas y personas que participaron en cada intervención. Evidencia: órdenes de trabajo, informes de mantenimiento, bitácoras, registros de fallas y actas de servicio.
- Restringir los privilegios de configuración de los equipos mediante políticas de administración centralizada, perfiles de usuario y permisos mínimos, limitando modificaciones sobre conexiones de red, usuarios locales, protector de pantalla, configuraciones del sistema y demás parámetros críticos; revisar periódicamente los privilegios asignados. Evidencia: matriz de permisos, políticas, configuraciones, logs y reportes de revisión.
- Configurar el bloqueo automático de las sesiones de usuario mediante políticas centralizadas del sistema operativo, estableciendo un tiempo máximo de cinco minutos de inactividad y verificando periódicamente su aplicación en las estaciones de trabajo. Evidencia: políticas de dominio, configuraciones de equipos, reportes de cumplimiento y resultados de pruebas.
- Restringir el almacenamiento local de información institucional mediante políticas de configuración que prioricen carpetas compartidas, OneDrive, SharePoint y demás repositorios institucionales autorizados, verificando periódicamente el cumplimiento y gestionando excepciones justificadas. Evidencia: políticas de configuración, reportes de almacenamiento, permisos, excepciones autorizadas y resultados de inspección.

- Implementar y monitorear estándares de hardening mediante líneas base de configuración para sistemas operativos, servidores, bases de datos, dispositivos de red, estaciones de trabajo y demás componentes tecnológicos, aplicándolas durante la implementación y revisándolas periódicamente y después de cambios relevantes. Evidencia: líneas base, checklists de hardening, reportes de cumplimiento, configuraciones, vulnerabilidades y planes de remediación.
- Identificar y evaluar los servicios de suministro que puedan afectar los activos de información mediante inventario de dependencias, análisis de criticidad, valoración de impacto y evaluación de riesgos, aplicando controles de mitigación y revisándolos periódicamente o ante cambios en el servicio. Evidencia: inventario de servicios, análisis de riesgos, matriz de controles, contratos, SLA y evaluaciones de proveedores.
- Ejecutar el borrado seguro de la información contenida en equipos antes de su reutilización, reasignación, devolución o disposición final mediante herramientas y procedimientos de eliminación segura acordes con el tipo de medio y sensibilidad de la información, verificando posteriormente que los datos no puedan ser recuperados. Evidencia: registros de borrado, certificados de eliminación, herramientas utilizadas, actas de disposición y resultados de verificación.
- Capacitar a los usuarios de computadores portátiles sobre transporte, custodia, protección física, conexión a redes, almacenamiento, bloqueo, reporte de incidentes y prevención de pérdida o robo, realizando la capacitación durante la entrega del equipo y actualizándola periódicamente. Evidencia: material de capacitación, registros de asistencia, evaluaciones y constancias de entrega del equipo.

Funcionarios y terceros de la entidad

- Utilizar los equipos y dispositivos institucionales exclusivamente para actividades relacionadas con las funciones o servicios autorizados mediante cuentas individuales, controles de acceso y políticas de uso aceptable, restringiendo el uso por terceros no autorizados y verificando periódicamente los eventos de uso cuando corresponda. Evidencia: políticas de uso aceptable, registros de acceso, logs y reportes de incumplimiento.
- Custodiar los equipos y elementos tecnológicos asignados mediante permanencia bajo control del usuario, bloqueo de sesión y almacenamiento seguro cuando no estén en uso, evitando dejarlos desatendidos en lugares de acceso público o no controlado. Evidencia: actas de entrega, inventario, inspecciones y reportes de pérdida o incidente.
- Asegurar los computadores portátiles mediante guayas de seguridad durante su utilización en espacios que presenten riesgo de sustracción y mediante almacenamiento bajo llave cuando no se disponga de guaya o el equipo permanezca sin supervisión. Evidencia: inventario de guayas, inspecciones físicas, registros de custodia y reportes de incidentes.
- Bloquear la sesión del equipo mediante el mecanismo de bloqueo del sistema operativo cada vez que el usuario se retire temporalmente de su puesto de trabajo. Evidencia: configuración de bloqueo automático, registros de inspección y reportes de cumplimiento.
- Apagar y asegurar los equipos mediante el procedimiento de apagado establecido durante ausencias prolongadas o al finalizar la jornada, exceptuando los casos en que deban permanecer encendidos para actividades remotas o procesos institucionales autorizados. Evidencia:

procedimiento, registros de excepciones y verificaciones de cumplimiento.

- Prevenir daños físicos y ambientales sobre equipos e información mediante la prohibición de alimentos, bebidas, humo, líquidos u otras prácticas que puedan generar deterioro, realizando verificaciones durante inspecciones de puestos de trabajo. Evidencia: listas de inspección, reportes de hallazgos, registros de mantenimiento e incidentes.
- Controlar las modificaciones de datos y configuraciones mediante cuentas individuales, permisos definidos y mecanismos de gestión de cambios, evitando intervenciones sobre equipos o información que no estén autorizadas y reportando cualquier modificación no reconocida. Evidencia: logs de acceso y modificación, solicitudes de cambio, tickets, matriz de permisos y registros de incidentes.

8.12.9. Seguridad de activos fuera de las instalaciones

Control Asociado en el MSPI: 7.9

Aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la entidad con el fin de mitigar la afectación a la confidencialidad, integridad y disponibilidad de los activos de información que sean retirados de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

Subdirección Gestión Administrativa

- Notificar la salida de equipos de cómputo mediante el canal institucional establecido, indicando como mínimo el activo, identificación, motivo, destino, período de salida y usuario encargado, antes de retirar el equipo de las instalaciones. Evidencia: correo, solicitud, autorización o registro de salida.

- Registrar cada activo de información retirado mediante el formato institucional de salida temporal de bienes, incorporando identificación y características del activo, estado físico, usuario encargado, destino, fecha de salida, fecha prevista de retorno y condiciones de devolución, antes de autorizar su retiro. Evidencia: formato de salida diligenciado, registro de autorización e inventario actualizado.
- Verificar el retorno de los activos retirados mediante la comparación entre el registro de salida, las características del activo y su estado físico, efectuando la actualización del inventario cuando se produzca la devolución y reportando las desviaciones identificadas. Evidencia: registro de devolución, acta de entrega, inventario actualizado y reporte de novedades.
- Aplicar medidas de protección física y lógica sobre los equipos y activos que permanezcan fuera de las instalaciones mediante controles de acceso, custodia, cifrado, autenticación, protección contra pérdida o robo y condiciones seguras de transporte y almacenamiento, ajustando las medidas al riesgo del entorno —trabajo de campo, entidades externas, residencia u otros— durante todo el período de permanencia fuera de la entidad. Evidencia: matriz de riesgos, listas de verificación, configuraciones de seguridad, registros de salida y reportes de inspección.

La SIDT

- Proteger los equipos portátiles, tabletas, discos duros y dispositivos de comunicaciones mediante elementos de seguridad física adecuados, tales como maletines, guayas, candados, cargadores, empaques, espumas y soportes, verificando su disponibilidad y estado antes de cada retiro de las instalaciones. Evidencia: lista de chequeo de salida,

inventario de elementos de protección, registro de entrega y fotografías cuando aplique.

- Deshabilitar los puertos y funcionalidades de infrarrojo y Bluetooth mediante políticas de configuración de los sistemas operativos y dispositivos de administración centralizada, manteniéndolos inactivos durante el período de uso cuando no exista una necesidad institucional justificada y autorizada. Evidencia: políticas de configuración, registros técnicos, reportes de cumplimiento y excepciones autorizadas.
- Aplicar controles de protección de confidencialidad sobre equipos portátiles que almacenen información reservada, clasificada o datos personales no públicos mediante cifrado de disco, autenticación robusta, bloqueo automático, control de privilegios y mecanismos de borrado o bloqueo remoto cuando estén disponibles, verificando su configuración antes de la salida y durante revisiones periódicas. Evidencia: configuración de cifrado, políticas de autenticación, reportes de cumplimiento, registros de administración y resultados de inspecciones.
- Validar las medidas de protección física y técnica de los equipos mediante la comparación de las condiciones de transporte, almacenamiento, operación y mantenimiento con las especificaciones y recomendaciones del fabricante, realizando la verificación antes de la salida y ante cambios de modelo, configuración o condiciones de uso. Evidencia: manuales y fichas técnicas, listas de verificación, conceptos técnicos, registros de mantenimiento y validaciones realizadas.

Seguridad de la Información

- Capacitar y sensibilizar a funcionarios y terceros sobre la custodia de activos retirados mediante instrucciones sobre transporte seguro, permanencia bajo supervisión, protección contra pérdida o robo, uso de

guayas y almacenamiento seguro, realizando la capacitación durante la entrega del activo y periódicamente o ante cambios en los controles. Evidencia: material de capacitación, registros de asistencia, evaluaciones y constancias de entrega.

- Sensibilizar sobre la protección de equipos portátiles durante desplazamientos mediante instrucciones para evitar su exposición dentro de vehículos y transportarlos como equipaje de mano durante viajes, reforzando estas prácticas durante las actividades de inducción, capacitación y campañas de seguridad. Evidencia: material de sensibilización, registros de asistencia, comunicaciones y resultados de campañas.
- Funcionarios y terceros de la entidad
- Reportar inmediatamente la pérdida o robo de un computador portátil mediante los canales institucionales establecidos, suministrando identificación del activo, ubicación aproximada, fecha y circunstancias del evento, y realizar la denuncia ante las autoridades competentes cuando corresponda, remitiendo posteriormente la constancia o copia de la denuncia. Evidencia: reporte de incidente, ticket, denuncia, comunicaciones y registro de bloqueo o acciones de protección ejecutadas.
- Reportar los eventos e incidentes relacionados con pérdida, daño, robo, alteración o compromiso de activos de información fuera de las instalaciones mediante los canales institucionales de gestión de incidentes, proporcionando información sobre el activo afectado, fecha, ubicación, circunstancias, información comprometida y evidencias disponibles, desde su identificación hasta el cierre del incidente. Evidencia: ticket de incidente, comunicaciones, fotografías o evidencias técnicas, análisis del incidente y registro de cierre.

8.12.10. Medios de almacenamiento

Control Asociado en el MSPI: 7.10

Establecer los procedimientos para la gestión de medios removibles para evitar posibles riesgos y fugas de la información y, con ello, proteger la información de usos no autorizados, robo, pérdida, uso indebido o corrupción de información en el proceso de transporte o transferencia de medios físicos. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Gestionar la disposición segura de medios de almacenamiento mediante procedimientos que establezcan la identificación, clasificación, retiro, reutilización, eliminación y destrucción de los medios, aplicando controles diferenciados según la sensibilidad de la información almacenada. Ejecutar el procedimiento antes de retirar, reutilizar o disponer cualquier medio que contenga información institucional. Evidencia: procedimiento vigente, registros de disposición, actas de entrega o destrucción y certificados correspondientes.
- Gestionar la disposición de residuos de aparatos eléctricos y electrónicos (RAEE) mediante mecanismos de recolección, almacenamiento temporal, entrega y disposición con gestores autorizados, de acuerdo con la normativa nacional aplicable. Para los discos duros y demás medios que contengan información, ejecutar previamente un proceso de borrado seguro y verificar su imposibilidad de recuperación; cuando el medio se encuentre dañado u obsoleto y no permita el borrado lógico, aplicar un método de destrucción física que impida la recuperación de la información. Evidencia: registros de disposición, certificados RAEE, reportes de borrado seguro, resultados de verificación y certificados de destrucción.

- Impedir la reutilización o comercialización de documentos destinados a reciclaje que hayan contenido información institucional mediante trituración, destrucción o tratamiento que imposibilite su reconstrucción antes de su entrega como material reciclable. Aplicar el control durante cada proceso de disposición documental. Evidencia: registros de destrucción, actas de disposición y certificados del proceso de reciclaje o destrucción.
- Controlar la copia no autorizada de información relevante mediante restricciones de acceso, permisos sobre repositorios, controles sobre dispositivos de almacenamiento y mecanismos de monitoreo de transferencia de información. Aplicar los controles de acuerdo con la clasificación de la información y durante cualquier proceso de copia o transferencia. Evidencia: configuraciones de permisos, registros de acceso, logs de transferencia, alertas y reportes de monitoreo.
- Registrar el ingreso y retiro de medios de almacenamiento que requieran transporte seguro mediante formatos de control que identifiquen el activo o medio, origen, destino, fecha y hora, persona encargada del transporte y entrega, condiciones físicas y medidas de protección aplicadas. Validar la autorización formal antes de retirar equipos, información o software de las instalaciones y actualizar el registro al momento de su devolución. Evidencia: autorizaciones, formatos de entrada/salida, registros de entrega y recepción, inventario y trazabilidad del transporte.
- Revisar los registros de retiro de activos mediante conciliaciones periódicas entre las autorizaciones, registros de salida e inventario institucional, identificando retiros no autorizados y determinando cuáles corresponden a medios de almacenamiento. Ejecutar la revisión con la periodicidad definida para el control de activos y ante hallazgos o

inconsistencias. Evidencia: informes de conciliación, inventarios, registros de salida, hallazgos y acciones correctivas.

- Reportar los eventos e incidentes asociados con pérdida, daño, robo o compromiso de activos durante su retiro mediante los canales institucionales de gestión de incidentes, registrando como mínimo el activo afectado, circunstancias, fecha, ubicación, información potencialmente comprometida y acciones realizadas. Reportar inmediatamente después de su identificación y realizar seguimiento hasta su cierre. Evidencia: ticket o reporte de incidente, comunicaciones, registros de bloqueo o recuperación, análisis y reporte de cierre.

La SIDT

- Restringir el uso y conexión de medios removibles mediante políticas de control de dispositivos, configuraciones centralizadas y mecanismos de autorización que permitan bloquear o habilitar USB, discos externos, memorias flash, dispositivos móviles y otros medios de almacenamiento. Aplicar la restricción por defecto y habilitar excepciones únicamente cuando exista una necesidad laboral previamente autorizada. Evidencia: políticas de configuración, inventario de dispositivos autorizados, registros de excepciones y logs de conexión.
- Controlar el uso de medios removibles autorizados mediante identificación del usuario, asignación individual, permisos de lectura/escritura y definición del propósito de utilización. Revisar periódicamente las autorizaciones y revocarlas cuando desaparezca la necesidad que las originó. Evidencia: matriz de autorizaciones, registros de asignación, configuraciones de seguridad y logs de uso.
- Bloquear la ejecución de programas provenientes de medios removibles mediante políticas de ejecución de aplicaciones, listas de permitidos y

controles de seguridad de los equipos. Permitir excepciones únicamente para software previamente validado y autorizado, verificando su integridad y seguridad antes de la ejecución. Evidencia: políticas de ejecución, listas de software autorizado, registros de excepciones, logs de ejecución y resultados de análisis de seguridad.

- Cifrar la información transferida mediante medios removibles utilizando mecanismos de cifrado aprobados institucionalmente y controles de autenticación para el acceso a la información. Aplicar el cifrado cuando la información tenga clasificación que lo requiera o cuando el riesgo de exposición durante el transporte lo justifique. Evidencia: configuración de cifrado, registros de transferencia, certificados o claves administradas y resultados de verificación.
- Restringir el almacenamiento de información pública clasificada, reservada, confidencial o datos personales en medios removibles mediante políticas de dispositivos, controles de acceso, cifrado y bloqueo de transferencia. Permitir excepciones únicamente cuando exista una necesidad justificada y autorización formal, aplicando medidas adicionales de protección. Evidencia: políticas DLP/control de dispositivos, autorizaciones, registros de transferencia, configuraciones y logs.
- Registrar la eliminación lógica o física de información contenida en medios removibles mediante un formato o herramienta que identifique el medio, motivo, tipo de eliminación, fecha, método utilizado y resultado de la verificación. Obtener aprobación previa cuando se requiera la eliminación total y realizar la copia de respaldo autorizada antes de ejecutar la eliminación, cuando corresponda. Evidencia: solicitud y aprobación, registro de eliminación, identificación del medio, copia de respaldo y resultado de la verificación.

- Verificar el análisis de medios removibles mediante la herramienta antivirus/antimalware institucional configurando el análisis automático al conectar el dispositivo y habilitando alertas ante detección de malware. Revisar periódicamente los resultados y atender las detecciones antes de permitir el acceso a la información o al dispositivo. Evidencia: configuración del antivirus, logs de análisis, alertas, reportes de detección y registros de tratamiento.
- Verificar la eliminación de información antes de reasignar un dispositivo mediante herramientas de borrado seguro y comprobaciones posteriores que permitan confirmar que la información anterior no puede ser recuperada. Ejecutar el procedimiento antes de cada reasignación, transferencia o reutilización del dispositivo. Evidencia: registro de borrado, herramienta utilizada, resultado de verificación, acta de reasignación y trazabilidad del activo.
- Aplicar desmagnetización, sobreescritura segura u otros métodos equivalentes a discos duros antes de su destrucción física mediante herramientas y procedimientos que impidan la recuperación de la información almacenada. Ejecutar el proceso antes de la destrucción cuando las condiciones técnicas del medio lo permitan. Evidencia: registro del proceso, método aplicado, resultado de verificación y acta de destrucción.
- Destruir físicamente los medios de almacenamiento mediante métodos que imposibiliten su reutilización y recuperación de información, tales como desintegración, pulverización, fundición, incineración o trituración; para medios ópticos, aplicar pulverización, trituración de corte transversal, incineración o método equivalente. Ejecutar la destrucción después del proceso de borrado seguro cuando este sea técnicamente posible. Evidencia: acta de destrucción, registro del medio, fotografías o

soportes del proceso y certificado de destrucción.

- Registrar la eliminación física de medios de almacenamiento mediante un mecanismo de trazabilidad que identifique el activo, motivo de eliminación, método aplicado, fecha, resultado y disposición final. Actualizar el registro inmediatamente después de cada proceso de destrucción y conciliarlo con el inventario de activos. Evidencia: registro de eliminación, acta de destrucción, certificado de disposición y actualización del inventario.

Seguridad de la Información

- Capacitar a funcionarios y terceros en el uso seguro de medios removibles mediante jornadas de inducción, reinducción, campañas y ejercicios prácticos sobre autorización, clasificación, cifrado, conexión, custodia, transferencia, eliminación y reporte de incidentes. Ejecutar la capacitación al ingreso y periódicamente, así como cuando se presenten cambios relevantes en las políticas o procedimientos. Evidencia: plan y material de capacitación, registros de asistencia, evaluaciones y resultados de campañas.
- Proporcionar mecanismos de cifrado para la protección de información en medios removibles mediante herramientas institucionales aprobadas, acompañadas de manuales e instrucciones para su instalación, configuración y utilización. Mantener estos recursos disponibles para las dependencias que requieran transferir información protegida y actualizar las herramientas cuando se presenten cambios tecnológicos o de seguridad. Evidencia: manuales publicados, inventario de herramientas, registros de entrega o habilitación, configuraciones de cifrado y soportes de actualización.

8.12.11. Servicios de apoyo

Control Asociado en el MSPI: 7.11

Proteger los equipos de cómputo y procesamiento contra fallas de energía u otras interrupciones causadas por fallas en los servicios de suministro. Por lo tanto, se desarrollarán las siguientes actividades:

Subdirección Gestión Administrativa

- Controlar el uso de la red de energía regulada mediante la identificación y señalización de los tomacorrientes destinados exclusivamente a computadores de escritorio, computadores portátiles y pantallas, manteniendo los demás equipos conectados a la red eléctrica no regulada. Verificar periódicamente el cumplimiento de la distribución establecida y corregir las conexiones no autorizadas. Evidencia: plano o esquema de redes eléctricas, señalización, registros de inspección y reportes de corrección.
- Regular y estabilizar el suministro eléctrico mediante UPS, reguladores, supresores de sobretensión, sistemas de protección eléctrica u otros mecanismos equivalentes, de acuerdo con la criticidad de los equipos y los riesgos identificados. Verificar su funcionamiento mediante pruebas periódicas y después de interrupciones o eventos eléctricos relevantes. Evidencia: inventario de equipos de protección, configuraciones, registros de mantenimiento, pruebas de funcionamiento e informes de inspección.
- Mantener sistemas de generación eléctrica de respaldo mediante plantas eléctricas dimensionadas de acuerdo con las cargas críticas de las sedes, realizando mantenimiento preventivo y correctivo conforme a las recomendaciones del fabricante y a los resultados de las inspecciones. Ejecutar pruebas periódicas de transferencia y operación para confirmar

su disponibilidad ante fallas del suministro principal. Evidencia: inventario, contratos de mantenimiento, hojas de vida de equipos, órdenes de servicio, certificados y resultados de pruebas.

- Incorporar controles para la continuidad de los servicios de suministro mediante procedimientos documentados que contemplen operación normal, interrupciones, contingencias, escalamiento, recuperación y coordinación con proveedores, integrándolos al Sistema de Gestión de Calidad. Revisar y actualizar los procedimientos ante cambios en la infraestructura, proveedores, riesgos o resultados de pruebas. Evidencia: procedimientos vigentes, registros de aprobación y actualización, matrices de controles, resultados de pruebas y registros del Sistema de Gestión de Calidad.
- Reportar eventos e incidentes asociados con fallas en los servicios de suministro mediante los canales institucionales de gestión de incidentes, registrando el servicio afectado, activo comprometido, fecha y hora, causa conocida, impacto y acciones ejecutadas. Realizar el reporte inmediatamente después de identificar el evento y efectuar seguimiento hasta su cierre. Evidencia: tickets, reportes de incidentes, comunicaciones con proveedores, registros de atención y análisis de cierre.
- Detectar oportunamente las fallas de los servicios públicos mediante sistemas de alarma, sensores, indicadores de estado o mecanismos equivalentes para monitorear energía, agua, climatización y demás servicios críticos. Configurar alertas y realizar pruebas periódicas para verificar su capacidad de detección y notificación. Evidencia: configuración de alarmas, registros de eventos, pruebas funcionales, alertas y reportes de monitoreo.
- Mantener condiciones de iluminación y comunicación durante

emergencias mediante sistemas de iluminación de respaldo y medios de comunicación alternos que permitan mantener la operación y facilitar la evacuación ante interrupciones de los servicios. Verificar su disponibilidad mediante pruebas periódicas y durante los ejercicios de emergencia. Evidencia: inventario de sistemas, registros de mantenimiento, pruebas de funcionamiento y resultados de simulacros.

- Ubicar los dispositivos de corte de servicios públicos en lugares accesibles y señalizados mediante la instalación de interruptores y válvulas de emergencia para energía, agua, gas y otros servicios, próximos a salidas de emergencia o salas de equipos, evitando su obstrucción. Verificar periódicamente su accesibilidad, identificación y funcionamiento. Evidencia: planos de ubicación, señalización, inspecciones, pruebas funcionales y registros de mantenimiento.
- Gestionar los contactos de emergencia mediante un directorio institucional protegido que contenga únicamente la información necesaria para establecer comunicación, como nombre y número telefónico. Mantener el directorio disponible para el personal autorizado y actualizarlo cuando se modifiquen los proveedores, contactos o mecanismos de atención. Evidencia: directorio vigente, registro de actualización, mecanismo de almacenamiento y control de acceso.
- Inspeccionar el funcionamiento de los servicios públicos mediante listas de verificación que contemplen suministro eléctrico, generación de respaldo, agua, climatización, comunicaciones y demás servicios necesarios para la operación. Realizar inspecciones periódicas y registrar las desviaciones para su tratamiento y seguimiento. Evidencia: listas de chequeo, informes de inspección, registros de mantenimiento, hallazgos y planes de acción.
- Verificar la disponibilidad de rutas alternativas de suministro mediante

la revisión de la infraestructura y documentación técnica de los proveedores, confirmando la existencia de múltiples alimentaciones y rutas físicas independientes cuando el servicio y su criticidad lo requieran. Realizar esta validación durante la contratación y periódicamente durante la prestación del servicio. Evidencia: documentación técnica del proveedor, planos de rutas, certificaciones, informes de verificación y cláusulas contractuales.

- Separar la infraestructura de apoyo de los servicios públicos de las redes de procesamiento de información mediante segmentación física o lógica, redes independientes, controles de acceso y restricciones de comunicación entre ambos ambientes. Verificar periódicamente la separación y revisar cualquier modificación de la arquitectura. Evidencia: diagramas de red, configuraciones de segmentación, reglas de firewall/ACL, pruebas de conectividad y registros de revisión.
- Verificar el estado operativo de los equipos asociados a los servicios públicos mediante inspecciones técnicas, reportes de operación y certificaciones de mantenimiento suministradas por los proveedores. Realizar la validación conforme a los intervalos establecidos por el fabricante y después de fallas o intervenciones, registrando las novedades y acciones correctivas. Evidencia: informes del proveedor, hojas de vida de equipos, certificados de mantenimiento, órdenes de servicio, resultados de inspección y registros de corrección.

8.12.12. Seguridad de cableado

Control Asociado en el MSPI: 7.12

Evitar pérdida, daño, robo o puesta en peligro de información y otros activos asociados, así como interrupción de operaciones de la organización relacionadas con el cableado de alimentación y comunicaciones. Por lo tanto, se desarrollarán las siguientes actividades:

Gestión Administrativa

- Implementar controles de seguridad para el cableado mediante procedimientos que contemplen identificación, protección física, organización, separación, inspección, mantenimiento y gestión de incidentes asociados al cableado eléctrico y de comunicaciones. Revisar y actualizar estos controles cuando se presenten cambios en la infraestructura, tecnología o riesgos identificados. Evidencia: procedimientos vigentes, planos, matrices de control, registros de inspección y mantenimiento.
- Incorporar los lineamientos de seguridad del cableado en los procedimientos del Sistema de Gestión de Calidad mediante la documentación de criterios técnicos para instalación, protección, organización, identificación, separación y mantenimiento. Verificar periódicamente su aplicación mediante inspecciones y listas de chequeo. Evidencia: procedimientos aprobados, listas de verificación, informes de inspección, registros de hallazgos y acciones correctivas.
- Reportar las fallas e incidentes relacionados con el cableado mediante los canales institucionales de gestión de incidentes, registrando el activo afectado, ubicación, tipo de daño, fecha, impacto y acciones ejecutadas. Realizar el reporte inmediatamente después de identificar la condición y efectuar seguimiento hasta su cierre. Evidencia: tickets, reportes de incidentes, registros fotográficos, órdenes de trabajo y reportes de cierre.
- Mantener la infraestructura física de los centros de cableado y centros de datos mediante inspecciones, mantenimiento preventivo y correctivo de puertas, cerraduras, paredes, pisos, techos, cielos rasos, pisos falsos, sistemas de climatización y demás elementos de protección física.

Ejecutar las actividades conforme al programa de mantenimiento y atender oportunamente las fallas identificadas. Evidencia: plan de mantenimiento, órdenes de trabajo, informes técnicos, registros de inspección y evidencias de corrección.

- Inspeccionar periódicamente el estado físico de los centros de cableado y centros de datos mediante listas de verificación que incluyan infraestructura, climatización, cerramientos, pisos, techos, puertas, cerraduras y condiciones ambientales. Registrar las novedades y generar solicitudes de mantenimiento para los daños identificados, realizando seguimiento hasta su corrección. Evidencia: listas de chequeo, informes de inspección, fotografías, solicitudes de mantenimiento y registros de cierre.
- Organizar e identificar el cableado de los racks y del cableado estructurado mediante etiquetado uniforme, rutas definidas, organizadores, bandejas, patch panels y documentación de las conexiones desde los puestos de trabajo hasta los centros de cableado. Verificar periódicamente la correspondencia entre el cableado instalado y la documentación técnica, especialmente después de modificaciones. Evidencia: diagramas de cableado, planos, inventario de conexiones, fotografías, etiquetado y registros de intervención.
- Proteger el cableado de comunicaciones y suministro eléctrico mediante canalizaciones, bandejas, ductos, cerramientos y mecanismos físicos que reduzcan el riesgo de interceptación, interferencia, manipulación accidental o daño. Inspeccionar las condiciones de protección periódicamente y después de intervenciones sobre la infraestructura. Evidencia: planos, especificaciones técnicas, registros de inspección, fotografías y órdenes de mantenimiento.
- Separar físicamente el cableado de comunicaciones del cableado

eléctrico mediante canalizaciones, bandejas o rutas independientes que reduzcan interferencias electromagnéticas y riesgos de seguridad. Verificar la separación durante la instalación, modificación o mantenimiento del cableado y mediante inspecciones periódicas. Evidencia: planos de rutas, especificaciones de instalación, registros de inspección, fotografías y actas de intervención.

La SIDT

- Controlar el ingreso y salida de personal a los centros de cableado y centros de datos mediante mecanismos de identificación, autorización, registro de visitantes y trazabilidad de entradas y salidas. Aplicar el control en cada acceso y revisar periódicamente los registros para detectar accesos no autorizados o inconsistencias. Evidencia: registros de acceso, controles electrónicos, autorizaciones, bitácoras y reportes de revisión.
- Autorizar y controlar el ingreso de personal externo a los centros de cableado y centros de datos mediante solicitud previa, validación de la necesidad de acceso, registro de ingreso, acompañamiento durante la actividad y registro de salida. Aplicar el control durante toda la permanencia del personal externo y documentar las actividades realizadas. Evidencia: solicitudes y autorizaciones, registros de visitantes, bitácoras de acompañamiento, órdenes de servicio y actas de intervención.
- Mantener restringido el acceso físico a los centros de cableado y centros de datos mediante puertas cerradas, cerraduras, controles de acceso, sistemas de autenticación y mecanismos de supervisión. Verificar periódicamente el funcionamiento de los controles y atender inmediatamente cualquier condición que permita acceso no autorizado.

Evidencia: registros de acceso, configuración de controles, inspecciones, reportes de mantenimiento y registros de incidentes.

- Controlar las actividades de aseo en los centros de cableado y centros de datos mediante un protocolo de limpieza que defina las condiciones de acceso, actividades permitidas, precauciones sobre equipos y cableado y acompañamiento durante la intervención. Verificar el cumplimiento durante cada jornada de aseo y registrar las novedades identificadas. Evidencia: protocolo de aseo, programación, listas de chequeo, bitácoras de acompañamiento y reportes de novedades.
- Gestionar el mantenimiento de los centros de cableado y centros de datos mediante un plan que contemple inspecciones preventivas, mantenimiento programado, atención de fallas, mejoras de infraestructura y seguimiento de acciones correctivas. Revisar y actualizar el plan periódicamente y después de incidentes, cambios tecnológicos o identificación de nuevas necesidades. Evidencia: plan de mantenimiento, cronogramas, órdenes de trabajo, informes técnicos, registros de fallas, acciones correctivas y evidencias de cierre.

8.12.13. Mantenimiento de equipo

Control Asociado en el MSPI: 7.13

Evitar pérdida, daño, robo o puesta en peligro de información y otros activos asociados, así como la interrupción de operaciones de la organización causada por la falta de mantenimiento. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Autorizar el acceso de contratistas o terceros a instalaciones o información mediante solicitud previa, validación de la actividad, alcance, vigencia, áreas y activos involucrados, asignando únicamente

los permisos requeridos. Aplicar la autorización antes de cada intervención y acompañar las actividades que impliquen acceso a infraestructura crítica o información sensible. Evidencia: solicitud y autorización de acceso, registro de visitantes, matriz de permisos, bitácora de acompañamiento y orden de servicio.

- Evaluar los riesgos de seguridad asociados a las actividades de mantenimiento de terceros mediante el análisis de la información, activos, instalaciones, accesos, amenazas, vulnerabilidades e impactos potenciales, definiendo controles de tratamiento proporcionales al riesgo identificado. Realizar la evaluación antes de iniciar actividades y actualizarla cuando cambien el alcance, los activos o las condiciones del servicio. Evidencia: matriz de riesgos, análisis de seguridad, plan de tratamiento y controles definidos.
- Determinar el alcance de acceso requerido por cada contratista o tercero mediante la identificación de instalaciones, equipos, sistemas, aplicaciones, redes e información necesarios para ejecutar el servicio, considerando su criticidad e impacto sobre las operaciones. Validar el alcance antes de autorizar el acceso y revisarlo cuando se modifique la actividad contratada. Evidencia: matriz de acceso, inventario de activos, solicitud de servicio y autorización.
- Clasificar el tipo de acceso requerido para actividades de mantenimiento mediante una matriz que diferencie acceso físico, lógico y de conectividad a redes, estableciendo para cada caso el alcance, duración, privilegios y controles de seguridad aplicables. Validar la clasificación antes de cada intervención y ante modificaciones del servicio. Evidencia: matriz de accesos, autorización, registros de configuración y bitácoras de intervención.
- Controlar el acceso físico de terceros mediante mecanismos de

identificación, registro de ingreso y salida, delimitación de áreas autorizadas y acompañamiento durante las actividades de mantenimiento. Aplicar los controles durante toda la permanencia del tercero en las instalaciones. Evidencia: registros de acceso, credenciales, bitácoras, autorizaciones y registros de acompañamiento.

- Controlar el acceso lógico de terceros mediante cuentas individuales, autenticación, perfiles basados en roles, mínimo privilegio, vigencia definida y registro de actividades. Habilitar los permisos únicamente durante el periodo autorizado y revocarlos al finalizar la intervención o cuando desaparezca la necesidad. Evidencia: solicitudes de acceso, matriz de permisos, configuraciones IAM/directorio, logs de autenticación y registros de revocación.
- Controlar la conectividad de terceros a las redes institucionales mediante segmentación, VLAN, firewall, ACL, VPN, canales dedicados u otros mecanismos de conexión segura, restringiendo las rutas, servicios, puertos y destinos permitidos. Aplicar las restricciones durante la intervención y revisar las configuraciones al finalizar el servicio. Evidencia: diagramas de red, reglas de firewall/ACL, configuración VPN, logs de conexión y pruebas de conectividad.
- Identificar el personal del contratista o tercero que tendrá acceso a información institucional mediante un registro actualizado que relacione nombre, empresa, función, servicio contratado, activos autorizados y periodo de acceso. Validar la información antes de habilitar cualquier acceso y actualizarla ante cambios de personal. Evidencia: listado de personal autorizado, certificaciones del proveedor, registros de acceso y solicitudes de modificación.
- Verificar los medios utilizados por terceros para almacenar, procesar, comunicar, compartir o intercambiar información mediante la revisión de

dispositivos, aplicaciones, canales de comunicación, mecanismos de almacenamiento y controles de protección empleados durante el servicio. Ejecutar la verificación antes de permitir el tratamiento de información y durante las evaluaciones de seguridad. Evidencia: inventario de medios, evaluación de seguridad, configuraciones, evidencias de cifrado y registros de transferencia.

- Aislar la conectividad de contratistas y terceros mediante una red segmentada y controles de firewall, ACL, autenticación y monitoreo que restrinjan la comunicación con redes donde se procese información confidencial o crítica. Mantener las restricciones durante toda la vigencia del acceso y verificar las reglas después de cada modificación. Evidencia: arquitectura de red, configuración de VLAN/firewall/ACL, logs de tráfico y pruebas de aislamiento.
- Incorporar las obligaciones legales, regulatorias y contractuales de seguridad y privacidad mediante cláusulas, anexos técnicos, acuerdos de confidencialidad y requisitos específicos de protección de información, acceso, tratamiento de datos, incidentes y devolución o eliminación de información. Validar su inclusión antes de la formalización del contrato y ante modificaciones contractuales. Evidencia: contrato, anexos, acuerdos de confidencialidad, matriz de requisitos y lista de verificación contractual.
- Gestionar el soporte y mantenimiento de los equipos tecnológicos mediante procedimientos que definan solicitud, diagnóstico, autorización, ejecución, pruebas, cierre y registro de cada intervención. Aplicar el procedimiento durante todo el ciclo de mantenimiento. Evidencia: procedimiento, tickets, órdenes de servicio, registros técnicos y actas de cierre.
- Registrar las actividades de mantenimiento preventivo y correctivo

mediante una herramienta o formato que identifique el activo, tipo de mantenimiento, fecha, técnico o proveedor, actividades ejecutadas, cambios realizados, resultados y estado final. Actualizar el registro inmediatamente después de cada intervención. Evidencia: historial de mantenimiento, tickets, órdenes de trabajo, informes técnicos y actualización del inventario.

- Programar anticipadamente el mantenimiento de servidores, comunicaciones, energía y demás componentes que puedan afectar la disponibilidad mediante un calendario de mantenimiento coordinado con las áreas involucradas, identificando impacto, duración, ventana autorizada, responsables técnicos, riesgos y plan de reversión. Notificar y autorizar las actividades antes de su ejecución. Evidencia: cronograma, solicitud de cambio, análisis de impacto, autorización, comunicaciones y acta de ejecución.
- Programar anticipadamente el mantenimiento de los equipos de cómputo mediante un cronograma basado en criticidad, recomendaciones del fabricante, estado del activo y necesidades operativas, coordinando ventanas de intervención que reduzcan la afectación del servicio. Actualizar el cronograma cuando se presenten cambios o mantenimientos extraordinarios. Evidencia: plan de mantenimiento, inventario, órdenes de servicio, cronograma y registros de ejecución.
- Autorizar la salida de equipos para reparación o mantenimiento externo mediante solicitud formal que identifique el activo, motivo, proveedor, destino, periodo de salida, información almacenada y controles de protección aplicables. Validar la autorización antes del retiro y registrar la devolución y estado del equipo. Evidencia: autorización de salida, formato de retiro, inventario, registro de entrega/recepción y acta de

devolución.

- Reportar eventos e incidentes relacionados con mantenimiento de equipos mediante los canales institucionales de gestión de incidentes, registrando activo afectado, tipo de evento, circunstancias, impacto, información comprometida y acciones ejecutadas. Realizar el reporte inmediatamente después de identificar la pérdida, daño, robo o compromiso y efectuar seguimiento hasta el cierre. Evidencia: ticket, reporte de incidente, registros técnicos, comunicaciones, análisis y cierre.
- Mantener los equipos conforme a las especificaciones del fabricante mediante planes de mantenimiento preventivo, actualización de firmware/software, reemplazo de componentes y aplicación de condiciones técnicas recomendadas. Ejecutar las actividades de acuerdo con los intervalos definidos por el fabricante y verificar su resultado después de cada intervención. Evidencia: manuales técnicos, hojas de vida, certificados, órdenes de mantenimiento, reportes técnicos y resultados de pruebas.
- Supervisar las actividades de mantenimiento realizadas por terceros en las instalaciones mediante acompañamiento, verificación del alcance autorizado, control de herramientas y equipos utilizados y validación de las actividades ejecutadas. Aplicar el control durante las intervenciones que involucren infraestructura, sistemas o información institucional. Evidencia: bitácoras de acompañamiento, listas de chequeo, órdenes de trabajo, informes de intervención y actas de cierre.
- Autorizar y controlar el mantenimiento remoto mediante solicitudes formales, autenticación individual, VPN o canales seguros, mínimo privilegio, vigencia temporal y monitoreo de las sesiones. Habilitar el acceso únicamente durante la ventana autorizada y revocarlo al finalizar

la actividad. Evidencia: solicitud y autorización, configuración VPN, matriz de permisos, logs de conexión, registros de sesión y evidencia de revocación.

- Aplicar controles de seguridad a los equipos retirados de las instalaciones para mantenimiento mediante cifrado, protección física, control de custodia, autorización de salida, transporte seguro y restricción de acceso a la información almacenada. Verificar los controles antes del retiro y confirmar el estado del activo al regresar. Evidencia: autorización de salida, lista de verificación, registro de custodia, inventario, acta de devolución y registros de cifrado.
- Gestionar la disposición o reutilización segura de equipos que hayan llegado al final de su vida útil mediante borrado seguro, sobreescritura, desmagnetización o destrucción física de los medios, de acuerdo con las características del dispositivo y la sensibilidad de la información. Ejecutar el proceso antes de su reutilización, transferencia o disposición final y verificar que la información no pueda ser recuperada. Evidencia: registro de borrado seguro, resultado de verificación, acta de destrucción o reutilización, certificado de disposición y actualización del inventario.

8.13. Componente Política de Seguridad de Redes

8.13.1. Protección contra "malware"

Control Asociado en el MSPI: 8.7

Garantizar protección de información y otros activos asociados contra "malware". Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Implementar mecanismos de protección contra software malicioso mediante soluciones antivirus, antimalware, antispyware y antispam

integradas a los equipos, servidores, correo electrónico y demás plataformas tecnológicas que lo requieran, configurando protección preventiva, detección, bloqueo y generación de alertas. Mantener los mecanismos activos durante toda la operación tecnológica y verificar periódicamente su cobertura. Evidencia: inventario de soluciones, consola de administración, políticas de seguridad, reportes de cobertura y registros de detección.

- Mantener actualizadas las soluciones de protección contra software malicioso mediante licencias vigentes y mecanismos automáticos o controlados de actualización del software, motores de detección, parches y bases de datos de firmas proporcionadas por el fabricante. Verificar periódicamente el estado de las licencias y actualizaciones y corregir oportunamente los equipos que presenten desactualización. Evidencia: licencias, certificados de autenticidad, reportes de versiones, estado de actualización, registros de parches y reportes de cumplimiento.
- Analizar la información almacenada y transmitida mediante las plataformas tecnológicas utilizando mecanismos de escaneo en tiempo real y bajo demanda sobre archivos, dispositivos, servidores, repositorios y servicios de correo electrónico. Ejecutar análisis automáticos y periódicos y generar alertas ante detecciones o fallas del mecanismo de protección. Evidencia: políticas de escaneo, logs, reportes de análisis, alertas y registros de eventos.
- Restringir la modificación de las configuraciones de seguridad mediante administración centralizada, perfiles de privilegios y controles de acceso que impidan a usuarios internos o externos deshabilitar, modificar o excluir componentes de antivirus, antimalware, antispyware y antispam. Revisar periódicamente los cambios de configuración y generar alertas ante modificaciones no autorizadas. Evidencia: políticas de

configuración, matriz de privilegios, logs de cambios, alertas y reportes de cumplimiento.

- Controlar las modificaciones de configuración de las estaciones de trabajo mediante políticas centralizadas para administrar conexiones de red, usuarios locales, servicios y parámetros críticos del sistema, restringiendo dichos cambios a cuentas administrativas autorizadas. Aplicar el control de forma permanente y registrar cada modificación realizada. Evidencia: políticas de configuración, perfiles administrativos, registros de cambios, logs y reportes de auditoría.
- Bloquear o detectar el acceso a sitios web maliciosos mediante listas de bloqueo, servicios de reputación, filtrado web, DNS seguro u otros mecanismos equivalentes, complementados con alertas ante intentos de conexión a dominios maliciosos. Actualizar las listas y reglas de protección periódicamente o cuando se identifiquen nuevas amenazas. Evidencia: listas de bloqueo, políticas de filtrado, registros DNS/web, alertas y reportes de sitios bloqueados.
- Revisar periódicamente el software y contenido de los sistemas que soportan procesos críticos mediante análisis de vulnerabilidades, integridad de archivos, versiones instaladas, configuraciones, código, componentes y contenido ejecutable. Ejecutar las revisiones de acuerdo con la criticidad del sistema y después de cambios relevantes o detección de amenazas. Evidencia: informes de análisis, inventarios de software, resultados de vulnerabilidades, registros de cambios y planes de remediación.
- Aislar las actividades de prueba de aplicaciones y programas mediante ambientes independientes de desarrollo, pruebas o laboratorio, separados lógica o físicamente de los ambientes productivos. Ejecutar las pruebas en estos ambientes antes de autorizar la implementación en

producción y controlar el acceso y los datos utilizados. Evidencia: diagramas de ambientes, configuraciones de segmentación, matrices de acceso, registros de pruebas y autorizaciones de paso a producción.

- Validar la seguridad de equipos externos antes de conectarlos a la red institucional mediante verificación de licenciamiento del software, estado de actualización, protección antivirus/antimalware y condiciones mínimas de seguridad definidas. Autorizar la conexión únicamente después de completar la validación y mantener controles de acceso durante el periodo de conexión. Evidencia: lista de chequeo, autorización de conexión, registros de validación, configuración de acceso y logs de red.
- Mantener actualizado el inventario de software autorizado mediante un catálogo institucional que registre nombre, versión, fabricante, finalidad, tipo de licencia y estado de autorización. Actualizar el catálogo ante nuevas adquisiciones, cambios de versión, retiro de software o identificación de aplicaciones no autorizadas. Evidencia: catálogo de software autorizado, inventario tecnológico, registros de actualización y reportes de software instalado.
- Validar las solicitudes de instalación de software mediante la comparación de la aplicación solicitada con el catálogo de software autorizado y la evaluación de aspectos de seguridad, licenciamiento, vulnerabilidades, compatibilidad y necesidad funcional. Ejecutar la validación antes de cada instalación y registrar las excepciones autorizadas. Evidencia: solicitud de instalación, concepto de validación, catálogo de software, evaluación de seguridad, autorización y ticket de instalación.

MANUAL OPERATIVO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Seguridad de la Información

- Sensibilizar sobre falsas alarmas y alertas de software malicioso mediante campañas, capacitaciones, casos prácticos y comunicaciones que expliquen cómo identificar, validar y reportar alertas sin deshabilitar los mecanismos de protección. Ejecutar las actividades periódicamente y ante cambios relevantes en las amenazas o mecanismos de protección. Evidencia: material de sensibilización, registros de asistencia, comunicaciones, evaluaciones y resultados de campañas.
- Gestionar información relacionada con software malicioso mediante la revisión de alertas, boletines técnicos, inteligencia de amenazas, reportes de fabricantes y fuentes confiables, utilizando esta información para actualizar controles y emitir comunicados de prevención o advertencia. Realizar la revisión periódicamente y ante amenazas de impacto relevante para la entidad. Evidencia: boletines analizados, registros de revisión, comunicados, alertas y actualizaciones de controles.
- Contener los incidentes asociados con software malicioso mediante aislamiento del equipo afectado, bloqueo de cuentas o conexiones, análisis técnico, eliminación de la amenaza, restauración y validación de los controles de protección. Activar las medidas inmediatamente después de confirmar el incidente y mantenerlas hasta verificar la recuperación segura del activo. Evidencia: ticket de incidente, alertas, logs, registros de aislamiento, análisis técnico, acciones de remediación y validación de recuperación.

Funcionarios y terceros

- Utilizar los equipos y recursos tecnológicos exclusivamente para actividades institucionales o contractuales autorizadas mediante asignación individual, autenticación personal, controles de acceso y políticas de uso aceptable. Aplicar las restricciones durante todo el periodo de asignación y registrar las excepciones formalmente autorizadas. Evidencia: acta de asignación, políticas de uso aceptable, registros de autenticación, controles de acceso y autorizaciones.
- Gestionar la instalación o modificación de software mediante la mesa de ayuda utilizando solicitudes formales que permitan validar la necesidad, licenciamiento, autorización y seguridad de la aplicación antes de su instalación. Aplicar el procedimiento para cada solicitud y conservar la trazabilidad de la intervención. Evidencia: ticket de mesa de ayuda, solicitud, validación, autorización y registro de instalación.
- Proteger las configuraciones de las herramientas de seguridad evitando su modificación, desactivación o eliminación y manteniendo los parámetros definidos institucionalmente. Reportar cualquier modificación accidental o alerta relacionada con la protección inmediatamente después de identificarla. Evidencia: políticas de seguridad, configuraciones centralizadas, logs de cambios, alertas y reportes de cumplimiento.
- Analizar los medios de almacenamiento antes de utilizarlos mediante las herramientas antivirus/antimalware institucionales y mecanismos de escaneo configurados para detectar archivos maliciosos. Ejecutar el análisis antes de abrir, copiar o ejecutar información proveniente de medios externos o fuentes no confiables. Evidencia: registros de escaneo, resultados del análisis, alertas y reportes de detección.
- Suspender el uso de un equipo cuando existan indicios de infección o falla que pueda comprometer la seguridad mediante la desconexión de

redes o aislamiento del dispositivo, evitando ejecutar, copiar o modificar información hasta realizar la evaluación técnica. Aplicar la medida inmediatamente después de detectar síntomas, alertas o comportamientos anómalos. Evidencia: reporte de incidente, alerta, registro de aislamiento, diagnóstico técnico y autorización de reincorporación.

- Controlar la descarga y ejecución de archivos provenientes de fuentes no confiables mediante filtros de navegación, protección de correo, análisis antivirus y validación del origen de los archivos antes de su apertura o ejecución. Aplicar el control especialmente a archivos recibidos por correo electrónico, sitios desconocidos y medios de almacenamiento externos. Evidencia: registros de navegación, logs de correo, alertas de seguridad, eventos antivirus y reportes de bloqueo.
- Reportar eventos e incidentes asociados con software malicioso o fallas de seguridad mediante los canales institucionales establecidos, registrando el activo afectado, alerta observada, comportamiento presentado, fecha, circunstancias y evidencias disponibles. Realizar el reporte inmediatamente después de identificar la sospecha y efectuar seguimiento hasta su tratamiento y cierre. Evidencia: ticket o reporte de incidente, capturas o evidencias técnicas, logs, análisis, acciones de contención y reporte de cierre.

8.13.2. Seguridad de redes

Control Asociado en el MSPI: 8.20

Proteger información en redes y sus instalaciones de procesamiento de información de apoyo contra el compromiso a través de la red. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Controlar el acceso a las redes de datos cableadas e inalámbricas mediante autenticación individual, perfiles de acceso, segmentación de red, control de dispositivos y asignación de permisos según rol y necesidad de negocio. Aplicar los controles durante todo el ciclo de vida del usuario y revisar periódicamente las autorizaciones. Evidencia: matriz de accesos, configuraciones de autenticación, registros de conexión, inventario de usuarios y reportes de revisión.
- Proteger las conexiones desde redes externas mediante VPN, IPSec, autenticación robusta, cifrado y reglas de firewall que restrinjan los servicios, direcciones y puertos autorizados. Aplicar los controles antes de habilitar cada conexión y revisarlos ante cambios de infraestructura, proveedor o nivel de riesgo. Evidencia: configuración VPN/IPSec, reglas de firewall, certificados, logs de conexión y pruebas de seguridad.
- Supervisar las actividades de terceros que accedan remotamente a la infraestructura mediante canales de conexión segura, autenticación individual, permisos temporales, mínimo privilegio y registro de las sesiones realizadas. Mantener el monitoreo durante toda la intervención y revocar los accesos al finalizarla. Evidencia: solicitud y autorización, registros de conexión, logs de sesión, bitácoras de actividad y evidencia de revocación.
- Monitorear el acceso y uso de los servicios informáticos mediante registros de autenticación, actividad, consumo y eventos de seguridad, aplicando reglas para detectar usos indebidos. Ante una actividad no autorizada o de alto riesgo, suspender o limitar el acceso según la criticidad y registrar el evento para su análisis. Evidencia: logs, alertas, tickets, registros de bloqueo o suspensión, análisis y comunicaciones.
- Autorizar y proteger las comunicaciones con entidades externas

mediante evaluación previa de la necesidad, clasificación de la información, canales dedicados o conexiones seguras a servicios cloud, autenticación, cifrado y restricciones de tráfico. Validar las configuraciones antes de habilitar la comunicación y revisarlas periódicamente. Evidencia: autorización, matriz de comunicación, diagramas de red, configuración de VPN/enlaces, reglas de firewall y logs.

- Administrar las identidades utilizadas en las redes mediante cuentas individuales, autenticación centralizada, perfiles por rol y controles que impidan el uso de cuentas, comunidades o contraseñas genéricas. Revisar periódicamente las cuentas existentes y eliminar o inhabilitar las que no tengan justificación. Evidencia: inventario de cuentas, matriz de roles, configuración de directorio/IAM, logs de autenticación y registros de depuración.
- Controlar los puertos físicos y lógicos de la infraestructura tecnológica mediante inventario, configuración segura y monitoreo de puertos utilizados, deshabilitando aquellos que no sean necesarios para la operación. Revisar la configuración periódicamente y después de cambios relevantes. Evidencia: inventario de puertos, configuraciones, resultados de escaneo, registros de cambios y reportes de revisión.
- Detectar intentos de intrusión y ataques contra las plataformas tecnológicas mediante IDS/IPS, firewall, SIEM, EDR u otras herramientas de monitoreo y correlación de eventos. Mantener las reglas de detección actualizadas y atender las alertas según su criticidad. Evidencia: alertas, logs, reglas de detección, tickets de incidentes, reportes de análisis y acciones de contención.
- Controlar el uso del servicio de Internet mediante filtrado web, categorías de navegación, autenticación, políticas de acceso y monitoreo

de tráfico, permitiendo únicamente actividades relacionadas con las funciones institucionales y contractuales. Revisar periódicamente los eventos de navegación y gestionar las excepciones autorizadas. Evidencia: políticas de navegación, reglas de filtrado, logs, reportes de uso y registros de excepciones.

- Controlar la publicación de información clasificada o reservada en sistemas colaborativos mediante reglas de clasificación, permisos de acceso, restricciones de compartición, revisión previa y mecanismos de prevención de fuga de información. Aplicar el control antes de publicar o compartir información y monitorear posteriormente su exposición. Evidencia: procedimiento, políticas de compartición, permisos, alertas DLP, registros de publicación y revisiones.
- Restringir el acceso móvil a servicios de computación en la nube mediante políticas de acceso condicional, autenticación multifactor, administración de dispositivos y validación del rol del usuario. Permitir el acceso únicamente cuando exista una necesidad laboral asociada a movilidad y se cumplan las condiciones de seguridad definidas. Evidencia: políticas de acceso condicional, registros MFA, inventario de dispositivos, autorizaciones y logs.
- Administrar las capacidades y permisos de los servicios cloud mediante roles, perfiles, cuotas, límites de consumo y principios de mínimo privilegio. Revisar periódicamente los permisos, capacidades asignadas y utilización de los servicios para ajustar los recursos cuando cambien las necesidades. Evidencia: matriz IAM, configuraciones cloud, reportes de consumo, revisiones de permisos y registros de cambios.
- Integrar al SIEM las actividades realizadas en sistemas colaborativos mediante conectores, APIs o mecanismos de recolección de logs que incorporen autenticaciones, cambios, accesos, comparticiones,

descargas y eventos administrativos. Mantener la integración activa y verificar periódicamente la recepción e integridad de los registros. Evidencia: configuración del conector, logs recibidos, dashboards SIEM, alertas y pruebas de integración.

- Bloquear el acceso a servicios cloud desde equipos o redes públicas mediante políticas de acceso condicional, validación de dispositivo, ubicación de conexión, autenticación multifactor y restricciones de red. Aplicar las restricciones durante el acceso y registrar los intentos bloqueados. Evidencia: políticas de acceso, registros de autenticación, logs de bloqueo y reportes de cumplimiento.
- Restringir la sincronización de información institucional con cuentas personales mediante políticas de identidad, administración de dispositivos, DLP y controles sobre aplicaciones de sincronización. Bloquear automáticamente las sincronizaciones no autorizadas y generar alertas para su revisión. Evidencia: políticas DLP, configuraciones de aplicaciones, logs de sincronización, alertas y reportes.
- Implementar mecanismos de autenticación para el acceso a la red mediante directorio institucional, autenticación individual, certificados, MFA u otros mecanismos definidos según el nivel de riesgo. Aplicar autenticación antes de permitir el acceso y registrar los eventos exitosos y fallidos. Evidencia: configuración de autenticación, políticas IAM, logs y reportes de acceso.
- Aislar temporalmente las subredes críticas mediante VLAN, ACL, firewall, cuarentena u otros mecanismos de segmentación cuando se identifiquen incidentes, amenazas o riesgos que puedan comprometer activos críticos. Mantener el aislamiento hasta completar el análisis y validar las condiciones para su reincorporación. Evidencia: solicitud o autorización de aislamiento, reglas de firewall/ACL, logs, análisis técnico y registro

de restitución.

- Deshabilitar protocolos de red vulnerables mediante evaluación técnica, análisis de vulnerabilidades, revisión de configuraciones y aplicación de políticas de seguridad que bloqueen protocolos inseguros o innecesarios. Ejecutar la deshabilitación cuando se confirme su vulnerabilidad o falta de necesidad y verificar posteriormente que no permanezcan activos. Evidencia: informe de vulnerabilidades, configuraciones, tickets de cambio, resultados de escaneo y pruebas de validación.
- Mantener actualizada la documentación de la infraestructura de red mediante control de versiones de diagramas, inventarios, direccionamiento, configuraciones y documentación técnica de los dispositivos. Actualizar la información después de cada cambio relevante y realizar una revisión periódica de consistencia. Evidencia: diagramas vigentes, archivos de configuración, inventarios, control de cambios y actas de revisión.

Seguridad de la Información

- Validar las solicitudes de conexión de terceros para soporte técnico mediante revisión de la necesidad, alcance, activo involucrado, tipo de acceso, duración, riesgos y controles requeridos antes de autorizar la conexión. Mantener la autorización limitada a la ventana y alcance definidos. Evidencia: solicitud, análisis de riesgo, autorización, matriz de acceso y registros de conexión.
- Evaluar los riesgos asociados al uso de servicios de computación en la nube mediante análisis de costos, disponibilidad, clasificación y sensibilidad de la información, ubicación de los datos, obligaciones legales y contractuales, dependencia del proveedor y controles disponibles. Realizar la evaluación antes de contratar o migrar

información y actualizarla ante cambios relevantes. Evidencia: matriz de riesgos, análisis de impacto, evaluación del proveedor, requisitos contractuales y plan de tratamiento.

- Monitorear la información almacenada, gestionada o desarrollada en servicios cloud mediante herramientas de auditoría, DLP, registros de actividad, controles de acceso y mecanismos de supervisión institucional, verificando el cumplimiento de las políticas de seguridad y privacidad. Ejecutar revisiones periódicas y ante incidentes o hallazgos relevantes. Evidencia: reportes de auditoría, logs, alertas, informes de monitoreo y registros de revisión.
- Jefes de las dependencias
- Clasificar la información destinada a servicios cloud mediante la aplicación de los criterios institucionales de confidencialidad, integridad, disponibilidad, sensibilidad y requisitos legales, determinando las condiciones de almacenamiento, intercambio y protección. Realizar la clasificación antes de almacenar o transferir información y actualizarla cuando cambie su naturaleza. Evidencia: inventario de información, matriz de clasificación, registros de revisión y autorizaciones.
- Asignar permisos sobre la información almacenada en la nube mediante matrices de acceso basadas en roles, funciones y necesidad de conocer, diferenciando permisos de lectura, edición, compartición y administración. Revisar periódicamente los permisos y ajustarlos ante cambios de funciones o usuarios. Evidencia: matriz de accesos, configuraciones de permisos, registros de revisión y logs de actividad.
- Gestionar la transferencia de grandes volúmenes de información desde la nube mediante un mecanismo previamente definido que contemple autorización, canal de transferencia, ubicación temporal, controles de acceso, integridad, disponibilidad y procedimiento de recuperación.

Aplicar el mecanismo cada vez que se requiera una transferencia masiva y verificar su resultado. Evidencia: solicitud, autorización, registros de transferencia, controles de acceso, validación de integridad y registro de recuperación.

Funcionarios y terceros

- Solicitar autorización para conexiones de terceros destinadas a soporte técnico mediante la mesa de ayuda o canal institucional definido, indicando tercero, equipo, servicio, motivo, alcance, periodo y tipo de acceso requerido. Gestionar la conexión únicamente después de obtener la autorización correspondiente. Evidencia: ticket, autorización, datos del tercero, registro de conexión y cierre de la intervención.
- Controlar el acceso y utilización de contenidos de Internet y servicios tecnológicos mediante filtros de navegación, controles de correo, políticas de uso aceptable y mecanismos de bloqueo que impidan contenidos ilícitos, ofensivos, maliciosos o contrarios a las disposiciones institucionales. Aplicar los controles de forma permanente y registrar los eventos que sean bloqueados o reportados. Evidencia: políticas, reglas de filtrado, logs, alertas y reportes de eventos.
- Impedir la publicación no autorizada de información institucional mediante el uso exclusivo de repositorios, sistemas colaborativos y servicios cloud aprobados, aplicando controles de acceso, clasificación y compartición. Verificar el destino antes de publicar o compartir información y reportar cualquier exposición accidental. Evidencia: configuración de repositorios, permisos, registros de publicación, alertas y reportes de incidentes.
- Identificar las opiniones expresadas en redes sociales personales como personales y no institucionales mediante una declaración explícita

cuando el contenido pueda asociarse con la entidad, evitando el uso de logotipos, cargos o elementos que puedan generar una representación institucional no autorizada. Aplicar esta condición en las publicaciones relacionadas con asuntos institucionales. Evidencia: lineamientos de uso de redes sociales, comunicaciones de sensibilización y registros de capacitación.

- Sincronizar los repositorios institucionales autorizados en la nube con equipos institucionales mediante mecanismos oficiales de sincronización y administración de dispositivos, verificando previamente que el equipo se encuentre vinculado al dominio institucional y cumpla las condiciones de seguridad requeridas. Aplicar la sincronización únicamente mediante cuentas institucionales autorizadas. Evidencia: configuración de sincronización, registro del dispositivo, políticas MDM/IAM y logs.
- Mantener depurada y actualizada la información almacenada en repositorios individuales cloud mediante revisión periódica de archivos, eliminación de información innecesaria, actualización de documentos y aplicación de las reglas de retención y clasificación. Ejecutar la revisión periódicamente y cuando cambien las necesidades de almacenamiento. Evidencia: registros de actividad, reportes de almacenamiento, controles de retención y revisiones de contenido.
- Mantener habilitado el control de cambios y las marcas de revisión en documentos colaborativos mediante las funcionalidades nativas de las plataformas autorizadas, permitiendo identificar modificaciones, versiones, usuarios y fechas. Mantener estos controles activos durante la elaboración y revisión de documentos que requieran trazabilidad. Evidencia: historial de versiones, registros de cambios, marcas de revisión y logs de actividad.
- Mantener habilitadas las funciones de seguimiento, revisión y auditoría

de los servicios cloud mediante políticas de configuración que impidan su desactivación por usuarios sin privilegios administrativos. Verificar periódicamente su estado y generar alertas ante intentos de modificación no autorizada. Evidencia: configuración de auditoría, logs, políticas administrativas, alertas y reportes de cumplimiento.

- Restringir el procesamiento o almacenamiento de información personal en servicios de colaboración no autorizados mediante políticas de clasificación, DLP, controles de compartición y bloqueo de aplicaciones o repositorios que no hayan sido aprobados institucionalmente. Aplicar el control durante todo el uso del servicio y ante cada intento de transferencia. Evidencia: políticas DLP, registros de transferencia, alertas, bloqueos y reportes de cumplimiento.
- Restringir la distribución de software no autorizado o ilegal mediante servicios cloud mediante controles de permisos, filtrado de archivos y políticas de uso que bloqueen o alerten sobre la distribución de software no permitido. Aplicar los controles de forma continua y gestionar las detecciones mediante el procedimiento de incidentes. Evidencia: políticas de seguridad, logs, alertas, registros de bloqueo y tickets.
- Prevenir intentos de acceso no autorizado o acciones que puedan afectar dispositivos, datos, cuentas o redes mediante autenticación, mínimo privilegio, controles de acceso, monitoreo y mecanismos de detección de actividades anómalas. Aplicar los controles permanentemente y bloquear o escalar las actividades que superen los criterios de riesgo establecidos. Evidencia: logs de autenticación, alertas, registros de bloqueo, análisis de eventos y tickets.
- Evitar actividades que degraden o impidan el uso de los servicios cloud por otros usuarios mediante límites de consumo, cuotas, controles de capacidad y monitoreo del uso de recursos. Detectar comportamientos

anómalos y aplicar restricciones cuando se afecte la disponibilidad del servicio. Evidencia: reportes de consumo, alertas de capacidad, logs y registros de intervención.

- Proteger el software y componentes disponibles en servicios cloud contra copias, modificaciones o manipulaciones no autorizadas mediante controles de acceso, permisos de edición, gestión de versiones y monitoreo de cambios. Revisar los cambios relevantes y atender cualquier modificación no autorizada mediante el proceso de incidentes. Evidencia: matriz de permisos, historial de versiones, logs de cambios, alertas y reportes de incidentes.
- Prevenir acciones que incrementen la vulnerabilidad de los servicios cloud o de la información almacenada mediante configuraciones seguras, mínimo privilegio, MFA, cifrado, segmentación, actualización de componentes y monitoreo continuo. Verificar periódicamente el cumplimiento de las configuraciones de seguridad y corregir las desviaciones identificadas. Evidencia: configuraciones de seguridad, informes de vulnerabilidades, resultados de auditoría, registros de cambios y planes de remediación.
- Reportar eventos que puedan constituir incidentes de seguridad o privacidad en sistemas de colaboración mediante los canales institucionales de reporte, registrando el servicio afectado, información involucrada, fecha, actividad observada y evidencias disponibles. Realizar el reporte inmediatamente después de identificar el evento y mantener la trazabilidad hasta su cierre. Evidencia: ticket de incidente, capturas o logs, alertas, comunicaciones, análisis técnico y reporte de cierre.

8.13.3. Seguridad de servicios de red

Control Asociado en el MSPI: 8.21

Garantizar la seguridad en el uso de servicios de red. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Registrar y conservar las actividades administrativas, operativas y de mantenimiento realizadas sobre equipos, servicios propios y servicios contratados, mediante mecanismos de trazabilidad, bitácoras y registros de auditoría, verificando su generación y disponibilidad de acuerdo con la criticidad del activo y ante actividades relevantes. Evidencia: registros de auditoría, bitácoras, reportes de actividad y resultados de revisión.
- Monitorear continuamente el desempeño y disponibilidad de los canales de comunicación mediante herramientas de supervisión de red, indicadores de capacidad, latencia, disponibilidad, pérdida de paquetes y utilización, estableciendo alertas cuando se presenten desviaciones frente a los niveles definidos. Evidencia: tableros de monitoreo, alertas, reportes de desempeño y registros de las acciones realizadas.
- Gestionar los niveles de servicio asociados a las actividades ejecutadas por contratistas y a los servicios tecnológicos requeridos por la entidad, mediante ANS/SLA, seguimiento de indicadores, gestión de requerimientos e incidentes y aplicación de acuerdos de escalamiento, realizando seguimiento durante la prestación del servicio. Evidencia: ANS/SLA, informes de cumplimiento, tickets, actas de seguimiento y registros de escalamiento.
- Controlar los puertos físicos y lógicos de las redes mediante mecanismos de autenticación, asignación, segmentación, listas de control de acceso,

VLAN, firewall y políticas de bloqueo, habilitando únicamente los puertos requeridos y revisando periódicamente los que se encuentren activos. Evidencia: configuraciones de red, inventario de puertos, reglas de firewall/ACL, registros de cambios y reportes de revisión.

- Verificar las medidas de seguridad implementadas por los proveedores de servicios de red mediante evaluaciones técnicas, revisión de configuraciones, informes de seguridad, certificaciones y evidencias de controles, antes de la prestación del servicio y periódicamente durante su vigencia o cuando se presenten cambios relevantes. Evidencia: informes de evaluación, certificaciones, listas de verificación, resultados de revisión y planes de tratamiento.
- Definir y aplicar los parámetros técnicos de conexión segura en coordinación con Seguridad de la Información, mediante estándares de autenticación, cifrado, protocolos seguros, direccionamiento, puertos, reglas de firewall, VPN y controles de acceso, antes de habilitar nuevas conexiones o modificar las existentes. Evidencia: matriz de parámetros técnicos, configuraciones, solicitudes aprobadas, diagramas de conexión y registros de pruebas.
- Restringir el acceso a las redes y servicios de red mediante el uso exclusivo de medios institucionales autorizados, como VPN, canales cifrados, autenticación individual y controles de acceso, bloqueando mecanismos de conexión no autorizados y verificando periódicamente las conexiones activas. Evidencia: configuración de VPN, registros de autenticación y conexión, reglas de firewall, inventario de accesos y reportes de revisión.
- Reportar oportunamente a Seguridad de la Información los eventos e incidentes que puedan comprometer activos de información a través de los servicios de red, mediante los canales institucionales de reporte y el

registro de la información técnica disponible, inmediatamente después de su detección o conocimiento. Evidencia: tickets o registros de incidentes, alertas, bitácoras, evidencias técnicas y comunicaciones de escalamiento.

8.13.4. Segregación de redes

Control Asociado en el MSPI: 8.22

Separar las redes, los grupos de servicios de información, sistemas de información y usuarios para controlar el tráfico entre ellos, en función de las necesidades misionales de la entidad. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Implementar y mantener la segregación de las redes de datos mediante segmentación física y lógica, VLAN, ACL, firewalls y reglas de enrutamiento, aislando los ambientes correspondientes a aplicaciones, servicios y dependencias según su nivel de criticidad y requerimientos de seguridad. Evidencia: diagramas de red, matriz de segmentación, configuraciones de VLAN/ACL/firewall y registros de cambios.
- Aislar el tráfico entre las zonas públicas y privadas mediante firewalls, ACL, reglas de filtrado y políticas de enrutamiento, permitiendo únicamente las comunicaciones expresamente autorizadas y revisando las reglas ante cambios en los servicios o la arquitectura de red. Evidencia: reglas de firewall, ACL, registros de tráfico, diagramas de segmentación y reportes de revisión.
- Segmentar la infraestructura de red en dominios físicos y lógicos independientes mediante VLAN, switches, equipos de enrutamiento y controles de seguridad, separando como mínimo las redes de usuarios

internos, visitantes, terceros, acceso a Internet y plataformas tecnológicas; revisar la segmentación periódicamente y ante cambios de infraestructura. Evidencia: diagramas de red, configuración de VLAN, tablas de enrutamiento, reglas de firewall y actas o reportes de revisión.

- Implementar y mantener una DMZ de Internet mediante firewalls y reglas de control de tráfico que restrinjan las conexiones entre Internet, la DMZ y las redes internas, autorizando únicamente los servicios, puertos y protocolos requeridos para la operación de las plataformas expuestas; revisar las reglas ante cambios, nuevas publicaciones o vulnerabilidades identificadas. Evidencia: arquitectura de red, configuración de la DMZ, reglas de firewall, matriz de puertos y reportes de revisión.
- Aislar la DMZ de las redes internas mediante segmentación lógica, firewalls y políticas de denegación por defecto, permitiendo únicamente los flujos de comunicación previamente autorizados por necesidad operacional y bloqueando cualquier acceso no requerido. Evidencia: reglas de firewall, ACL, registros de tráfico bloqueado/permitido, pruebas de conectividad y reportes de validación.
- Separar las redes alámbricas e inalámbricas mediante segmentación física o lógica, VLAN, SSID diferenciados y políticas de acceso, habilitando redes inalámbricas públicas únicamente para visitantes o situaciones autorizadas y evitando su comunicación directa con las redes internas. Evidencia: configuración de switches y puntos de acceso, VLAN/SSID, reglas de firewall y pruebas de aislamiento.
- Proteger los dominios de red internos frente a Internet mediante firewalls, NAT, ACL, filtrado de tráfico y reglas de comunicación entre zonas, restringiendo las conexiones entrantes y salientes a los servicios y destinos autorizados y revisando las políticas periódicamente.

Evidencia: configuración de firewall, reglas NAT/ACL, registros de tráfico y reportes de revisión.

- Controlar el acceso inalámbrico de invitados mediante portal cautivo, autenticación, aceptación de condiciones de uso, segmentación de la red y políticas de filtrado, manteniendo el tráfico de visitantes aislado de la infraestructura interna y aplicando restricciones equivalentes a las definidas para el uso institucional de Internet; revisar los controles cuando se modifiquen las condiciones del servicio. Evidencia: configuración del portal cautivo, registros de autenticación, políticas de acceso, configuración de VLAN/firewall y reportes de pruebas de aislamiento.
- Implementar una red aislada para los equipos de análisis forense mediante segmentación dedicada, VLAN, firewall y controles de autenticación, restringiendo el acceso exclusivamente a los usuarios autorizados de Fiscalización (TACI) y evitando la comunicación no requerida con las demás redes institucionales. Evidencia: diagrama de red forense, matriz de accesos, configuración de VLAN/firewall, registros de autenticación y pruebas de aislamiento.
- Reportar oportunamente a Seguridad de la Información los eventos o incidentes relacionados con el compromiso de activos de información a través de los servicios de red, utilizando los canales institucionales de reporte y conservando las evidencias técnicas disponibles, inmediatamente después de su detección o conocimiento. Evidencia: tickets o registros de incidentes, alertas, logs de red, evidencias técnicas y comunicaciones de escalamiento.

8.13.5. Filtro Web

Control Asociado en el MSPI: 8.23

Administrar el acceso a sitios web en los equipos de la ANCP-CCE con el fin de reducir la exposición a contenido malicioso, afectación a los servicios de red, acceso a contenido ilegal y similares. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Gestionar y actualizar las reglas para el uso seguro y apropiado de los recursos en línea mediante políticas de navegación, criterios de filtrado, categorías de sitios web y restricciones sobre aplicaciones web, revisándolas como mínimo una vez al año y cuando se presenten cambios tecnológicos, regulatorios o nuevas amenazas. Evidencia: política de navegación vigente, matriz de categorías y restricciones, historial de cambios y registros de aprobación.
- Incorporar en las reglas de navegación criterios diferenciados para equipos conectados a la red institucional y equipos utilizados en teletrabajo, mediante políticas de acceso, filtrado, protección del endpoint y controles de conexión remota, aplicándolos de acuerdo con el tipo de conexión y nivel de riesgo. Evidencia: política de navegación, configuración de controles para equipos institucionales y teletrabajo, y resultados de verificación.
- Clasificar y documentar los tipos de sitios y servicios web permitidos, restringidos o sujetos a autorización mediante una matriz de categorías de navegación basada en riesgo, función institucional y clasificación de la información, actualizándola cuando se identifiquen nuevas amenazas o necesidades operativas. Evidencia: matriz de categorías web, criterios de clasificación, historial de actualización y aprobaciones.

- Evaluar las solicitudes de acceso a sitios o servicios restringidos mediante la validación de la necesidad institucional, justificación de uso, riesgo de seguridad y vigencia de la solicitud, autorizando o rechazando el acceso antes de modificar las restricciones de navegación. Evidencia: solicitud de excepción, análisis de riesgo, autorización o rechazo y registro de la decisión.
- Definir y mantener controles de restricción de navegación mediante categorías de filtrado, listas de bloqueo, inteligencia de amenazas, reputación de dominios/IP y mecanismos de protección contra malware y phishing, actualizándolos ante la identificación de nuevas amenazas. Evidencia: política de filtrado, listas de bloqueo, configuración de las herramientas y reportes de actualización.
- Bloquear el acceso a sitios con capacidad de carga de información mediante controles de filtrado y reglas de navegación, excepto cuando exista una necesidad misional previamente autorizada y se hayan aplicado los controles de seguridad correspondientes. Evidencia: reglas de filtrado, excepciones autorizadas, registros de acceso y logs de navegación.
- Bloquear sitios web maliciosos o sospechosos mediante listas de reputación, inteligencia de amenazas, análisis de URL/dominio e integración con herramientas de seguridad, actualizando las fuentes de detección de acuerdo con la frecuencia definida por las herramientas o ante nuevas amenazas. Evidencia: listas de bloqueo, alertas, reportes de inteligencia de amenazas y registros de navegación.
- Restringir el acceso a servidores de mando y control (C2) mediante listas de indicadores de compromiso, inteligencia de amenazas, filtrado DNS/URL y controles de firewall o seguridad perimetral, aplicando el bloqueo inmediatamente después de identificar un indicador como

malicioso. Evidencia: IOC registrados, reglas de bloqueo, alertas de seguridad y logs de conexiones bloqueadas.

- Bloquear dominios, direcciones IP y sitios identificados como maliciosos mediante inteligencia de amenazas, utilizando fuentes confiables, indicadores de compromiso y mecanismos automatizados o administrados de actualización, revisando su vigencia periódicamente. Evidencia: fuentes de inteligencia utilizadas, listas de bloqueo, registros de actualización y reportes de aplicación.
- Restringir el acceso a sitios que distribuyan o compartan contenido ilegal mediante categorías de filtrado web y listas de bloqueo, incorporando nuevos indicadores cuando sean identificados por las fuentes institucionales, legales o de seguridad correspondientes. Evidencia: categorías configuradas, listas de bloqueo, registros de actualización y reportes de filtrado.
- Verificar como mínimo una vez al año la aplicación efectiva de los filtros web mediante pruebas controladas sobre categorías permitidas, restringidas y bloqueadas, revisión de configuraciones y análisis de registros, documentando las desviaciones y aplicando las correcciones necesarias. Evidencia: plan de pruebas, resultados, capturas o registros de validación, hallazgos y acciones correctivas.
- Capacitar a funcionarios y terceros sobre el uso seguro de los recursos en línea mediante inducciones, capacitaciones, campañas de sensibilización y material institucional, incluyendo las reglas de navegación, canales de reporte y procedimiento para solicitar excepciones; realizar la capacitación durante la vinculación y periódicamente según el plan de sensibilización. Evidencia: plan de capacitación, material utilizado, registros de asistencia, evaluaciones y comunicaciones realizadas.

- Comunicar las reglas de navegación segura mediante políticas, instructivos, campañas y medios institucionales, incluyendo las restricciones aplicables, conductas esperadas y consecuencias del uso indebido; actualizar la información cuando se modifiquen las reglas. Evidencia: publicaciones, comunicaciones, instructivos y registros de divulgación.
- Informar los canales para reportar problemas de seguridad mediante capacitaciones, intranet, procedimientos y material de sensibilización, manteniendo la información disponible y actualizada para funcionarios y terceros. Evidencia: procedimientos publicados, material de capacitación y registros de divulgación.
- Gestionar las excepciones de navegación mediante un procedimiento formal de solicitud, justificación, evaluación de riesgo, autorización, vigencia y revisión, aplicándolo cada vez que se requiera acceder a un recurso web restringido por necesidad institucional. Evidencia: solicitudes, análisis de riesgo, autorizaciones, vigencia de excepciones y registros de revisión.

La SIDT

- Implementar las restricciones definidas para la navegación web mediante políticas de firewall, proxy, DNS, filtros URL, listas de bloqueo y controles de seguridad de los endpoints, bloqueando las direcciones IP, dominios o categorías identificadas y actualizando las reglas cuando Seguridad de la Información modifique los criterios. Evidencia: configuraciones de seguridad, listas de bloqueo, registros de cambios y logs de navegación.
- Canalizar las solicitudes de acceso a sitios o servicios restringidos mediante el mecanismo institucional de solicitudes y su remisión a

Seguridad de la Información para evaluación, evitando habilitar accesos sin la autorización correspondiente. Evidencia: tickets o solicitudes, trazabilidad de remisión, autorización o rechazo y registros de configuración.

- Bloquear el acceso a páginas, portales, sitios y aplicaciones web no autorizados mediante la política institucional de navegación y los controles tecnológicos de filtrado, aplicando las restricciones de acuerdo con la clasificación de categorías y verificando su efectividad mediante registros de navegación. Evidencia: política de navegación, configuración de filtros, logs de acceso/bloqueo y reportes de monitoreo.

Funcionarios y terceros de la entidad

- Solicitar el acceso a páginas o servicios de Internet restringidos mediante el canal institucional definido, con la validación previa del jefe inmediato, indicando la necesidad, recurso solicitado, justificación y tiempo requerido, cada vez que el acceso sea necesario para desarrollar actividades institucionales. Evidencia: solicitud registrada, autorización del jefe inmediato, justificación y respuesta de Seguridad de la Información.
- Utilizar los recursos web institucionales conforme a las restricciones establecidas, mediante los mecanismos de autenticación, filtrado y monitoreo implementados, absteniéndose de utilizar mecanismos para evadir los controles de navegación y reportando inmediatamente cualquier evento de seguridad identificado. Evidencia: registros de navegación, alertas de seguridad, reportes de incidentes y registros de atención.

8.14. Componente Política de Seguridad de Configuraciones

8.14.1. Gestión de configuración

Control Asociado en el MSPI: 8.9

Establecer, documentar, implementar, socializar, monitorear y revisar las configuraciones de seguridad, de hardware, software, servicios y redes para permitir que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida y que la configuración no se altere por cambios no autorizados o incorrectos. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Diseñar y mantener plantillas de configuración segura para equipos de cómputo, hardware, software, sistemas operativos, servicios tecnológicos, servicios en la nube y componentes de red, mediante líneas base de seguridad que incorporen parámetros de autenticación, privilegios, servicios habilitados, protocolos, puertos, registros, actualizaciones y controles de protección, aplicándolas durante la instalación, puesta en producción y vida útil de los activos. Evidencia: plantillas aprobadas, líneas base de seguridad, listas de verificación y registros de aplicación.
- Controlar los cambios de configuración mediante procedimientos de gestión de cambios, segregación de funciones, autorización previa, evaluación de impacto, pruebas, implementación controlada y registro de reversión, aplicándolos antes de modificar configuraciones de hardware, software, servicios o redes. Evidencia: solicitudes y registros de cambio, aprobaciones, resultados de pruebas, bitácoras y planes de reversión.
- Reducir las cuentas con privilegios administrativos mediante matrices de

roles y permisos, principio de mínimo privilegio, cuentas individuales y mecanismos de gestión de acceso privilegiado, revisando periódicamente los privilegios asignados y retirando aquellos que no sean necesarios. Evidencia: matriz de accesos, inventario de cuentas privilegiadas, registros de revisión y reportes de acceso.

- Deshabilitar o eliminar identidades innecesarias, inactivas o inseguras mediante revisiones periódicas de cuentas, controles de directorio y mecanismos automatizados de bloqueo o desactivación, aplicando la medida cuando una cuenta deje de ser requerida, presente riesgo o no cumpla las condiciones de seguridad. Evidencia: reportes de cuentas, registros de desactivación, tickets y resultados de revisión.
- Deshabilitar o restringir funciones, puertos y servicios innecesarios mediante líneas base de endurecimiento, listas de servicios autorizados, políticas de firewall y controles de configuración, aplicando el principio de mínima funcionalidad durante la instalación y ante cambios tecnológicos. Evidencia: líneas base, configuraciones, inventarios de servicios/puertos y resultados de verificación.
- Integrar la gestión de configuración con la gestión de activos mediante la asociación de cada configuración, línea base y cambio con el activo correspondiente en las herramientas institucionales, actualizando los registros cada vez que se incorpore, modifique, retire o reconfigure un activo. Evidencia: inventario de activos, registros de configuración, CMDB o herramienta equivalente y trazabilidad de cambios.
- Proteger las plantillas y líneas base de configuración mediante controles de acceso, permisos restringidos, almacenamiento seguro, control de versiones y registro de modificaciones, revisando periódicamente los accesos y evitando su consulta o alteración por usuarios no autorizados. Evidencia: permisos de acceso, historial de versiones, registros de

auditoría y repositorio protegido.

- Definir y aplicar configuraciones de seguridad para equipos propiedad de proveedores que almacenen, procesen o transmitan información de la ANCP-CCE mediante requisitos contractuales, líneas base, controles de acceso, cifrado, protección contra malware, actualización de software y restricciones de uso, verificando su cumplimiento antes de permitir el procesamiento de información institucional y durante la prestación del servicio. Evidencia: cláusulas contractuales, listas de verificación, configuraciones verificadas, certificaciones y reportes de supervisión.
- Revisar y actualizar preventivamente las plantillas de configuración segura mediante análisis de vulnerabilidades, alertas de seguridad, recomendaciones de fabricantes, cambios tecnológicos y resultados de incidentes, realizando la actualización cuando se identifiquen nuevas amenazas o recomendaciones relevantes y como mínimo durante la revisión periódica definida. Evidencia: versiones actualizadas de las plantillas, informes de vulnerabilidades, recomendaciones de fabricantes, registros de cambios y aprobaciones.
- Aplicar las configuraciones de seguridad definidas mediante herramientas de gestión centralizada, políticas de dominio, sistemas de administración de endpoints, automatización, herramientas de configuración y controles de infraestructura, verificando la aplicación de la línea base durante la instalación y después de cambios significativos. Evidencia: reportes de cumplimiento, configuraciones aplicadas, políticas, logs de administración y resultados de validación.
- Monitorear periódicamente la configuración de hardware, software, servicios y redes mediante herramientas de gestión de configuración, escaneo de cumplimiento, monitoreo de endpoints y análisis de desviaciones frente a las líneas base, generando alertas y acciones

correctivas cuando se detecten configuraciones no autorizadas. Evidencia: reportes de cumplimiento, alertas de desviación, tickets de remediación y resultados de verificación.

- Restringir las modificaciones de configuración mediante cuentas administrativas individuales, control de acceso basado en roles, mínimo privilegio y mecanismos de autenticación reforzada, permitiendo cambios únicamente a usuarios autorizados y registrando toda modificación mediante el procedimiento de gestión de cambios. Evidencia: matriz de privilegios, registros de autenticación, logs de configuración, tickets y aprobaciones de cambio.
- Aplicar controles de gestión de cambios a las configuraciones de seguridad mediante evaluación de impacto, análisis de riesgos, pruebas previas, autorización, ventana de implementación, documentación y validación posterior, cada vez que se modifique una configuración que pueda afectar la seguridad, disponibilidad o funcionamiento del activo. Evidencia: solicitud de cambio, análisis de impacto, aprobación, resultados de pruebas, bitácora de implementación y validación posterior.
- Medir la gestión de vulnerabilidades asociada a las configuraciones mediante indicadores diferenciados por nivel de severidad, activos afectados, tiempos de remediación, vulnerabilidades abiertas y porcentaje de cumplimiento, realizando el seguimiento con la periodicidad definida para el SGSI y priorizando las vulnerabilidades críticas y altas. Evidencia: tablero de indicadores, informes de vulnerabilidades, métricas de remediación, tendencias y planes de tratamiento.
- Reportar oportunamente a Seguridad de la Información los eventos e incidentes relacionados con pérdida, daño, robo o compromiso de activos

derivados de fallas de configuración, mediante los canales institucionales de reporte y el registro de las evidencias técnicas disponibles, inmediatamente después de su detección o conocimiento. Evidencia: tickets de incidente, alertas, logs, evidencias técnicas, comunicaciones de escalamiento y registros de atención.

8.14.2. Uso de criptografía

Control Asociado en el MSPI: 8.24

Garantizar uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos empresariales, de seguridad de la información y teniendo en cuenta requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía. Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Validar la aplicación del cifrado sobre información pública reservada y clasificada, así como datos personales sensibles, privados, semiprivados y de menores, mediante revisiones de configuraciones, pruebas técnicas y verificación de los mecanismos criptográficos utilizados durante el almacenamiento y la transmisión, de forma periódica y ante cambios relevantes en los sistemas. Evidencia: informes de validación, resultados de pruebas, configuraciones y registros de cumplimiento.
- Establecer y mantener los lineamientos de uso de criptografía mediante criterios de clasificación de información, niveles de protección, algoritmos y protocolos autorizados, gestión de claves, certificados y condiciones de aplicación, revisándolos periódicamente y cuando cambien los riesgos, tecnologías o requisitos normativos. Evidencia: lineamientos criptográficos aprobados, matriz de controles y registros de

actualización.

- Aplicar condiciones de cifrado al correo electrónico mediante configuración de cifrado de mensajes, archivos adjuntos y canales de transmisión, cuando se envíe información pública reservada o clasificada, verificando su aplicación antes de la transmisión. Evidencia: configuración de correo, políticas de cifrado, registros de transmisión y resultados de pruebas.

La SIDT

- Proteger las contraseñas y claves de acceso almacenadas en sistemas y aplicaciones mediante hashing, cifrado, gestores de secretos u otros mecanismos criptográficos aprobados, evitando el almacenamiento en texto plano y verificando su implementación durante las pruebas de seguridad y revisiones periódicas. Evidencia: configuraciones, resultados de análisis de código, pruebas de seguridad y reportes de cumplimiento.
- Identificar los sistemas y aplicaciones que transmiten información pública reservada o clasificada mediante inventario de activos, clasificación de información y análisis de flujos de datos, aplicando mecanismos de cifrado antes de habilitar la transmisión y ante cambios en los flujos de información. Evidencia: inventario, matriz de clasificación, diagramas de flujo y configuraciones de cifrado.
- Cifrar los discos de los equipos que almacenen información pública reservada o clasificada mediante mecanismos de cifrado de disco administrados centralmente, verificando periódicamente el estado de protección y aplicándolo antes de almacenar información clasificada. Evidencia: reportes de cifrado, inventario de equipos protegidos y registros de cumplimiento.
- Proteger los canales de comunicación internos y externos mediante

protocolos seguros, certificados digitales y algoritmos criptográficos aprobados, configurándolos durante la implementación de los servicios y revisándolos periódicamente frente a vulnerabilidades o cambios tecnológicos. Evidencia: configuraciones, certificados, inventario de protocolos y resultados de pruebas de seguridad.

- Proteger las conexiones VPN con terceros mediante autenticación robusta, cifrado de extremo a extremo, certificados o llaves, segmentación y restricciones de acceso, habilitando las conexiones únicamente después de validar los parámetros de seguridad y revisándolos cuando cambie el tercero, servicio o riesgo. Evidencia: configuración VPN, matriz de accesos, certificados, logs de conexión y resultados de pruebas.
- Implementar mecanismos de firma electrónica y criptografía en servicios institucionales como gestión documental, expedientes electrónicos, sede electrónica, automatización de procesos, comunicaciones y servicios digitales, mediante soluciones tecnológicas que proporcionen autenticidad, integridad y no repudio, priorizando su implementación según criticidad y necesidades del servicio. Evidencia: diseños técnicos, configuraciones, certificados, registros de firma y resultados de pruebas.
- Cifrar la información clasificada durante su recepción, almacenamiento, transmisión y consulta mediante controles criptográficos aplicados a bases de datos, aplicaciones, dispositivos de almacenamiento y canales de comunicación, activándolos de acuerdo con la clasificación y nivel de riesgo de cada activo. Evidencia: configuraciones, matrices de protección, resultados de pruebas y reportes de cumplimiento.
- Aplicar firmas digitales, firmas electrónicas y mecanismos criptográficos mediante certificados, llaves y servicios de validación autorizados, utilizándolos en transacciones que requieran autenticidad, integridad y

no repudio y verificando la validez de las firmas durante el procesamiento. Evidencia: certificados, registros de firma, trazabilidad de transacciones y resultados de validación.

- Aplicar controles criptográficos durante todo el ciclo de vida de documentos y archivos digitales mediante cifrado, firmas, controles de acceso y gestión segura de claves, desde su creación o recepción hasta su almacenamiento, transferencia, consulta, archivo y eliminación, cuando contengan información protegida. Evidencia: configuraciones, registros de acceso, evidencias de cifrado y controles de disposición.
- Proteger la información de intercambio tributario, aduanero y cambiario mediante canales cifrados, autenticación robusta, segmentación y esquemas de seguridad independientes, aplicando los controles durante la recepción, almacenamiento, consulta y transmisión. Evidencia: configuraciones de seguridad, registros de intercambio, certificados y resultados de pruebas.
- Generar y conservar valores hash o sumas de verificación mediante algoritmos criptográficos aprobados, calculándolos al recibir, transferir o almacenar información cuya integridad deba verificarse y comparándolos posteriormente cuando se requiera validar que no ha sido alterada. Evidencia: valores hash registrados, algoritmos utilizados, registros de comparación y resultados de validación.
- Autenticar usuarios y entidades externas mediante certificados digitales, infraestructura de llave pública, autenticación criptográfica u otros mecanismos equivalentes, aplicándolos de acuerdo con la criticidad del servicio y los lineamientos institucionales. Evidencia: certificados, registros de autenticación, configuraciones y logs de acceso.
- Administrar las herramientas y mecanismos criptográficos mediante configuración centralizada, control de acceso, gestión de versiones,

monitoreo y registro de actividades administrativas, verificando periódicamente su funcionamiento y estado de seguridad. Evidencia: inventario de soluciones, configuraciones, logs administrativos y reportes de revisión.

- Implementar cifrado en dispositivos de almacenamiento y bases de datos mediante cifrado de discos, bases de datos, tablespaces y medios de almacenamiento, aplicándolo según la clasificación de la información y verificando periódicamente su estado de protección. Evidencia: configuraciones de cifrado, reportes de cumplimiento y resultados de pruebas.
- Verificar la aplicación de controles criptográficos en sistemas desarrollados internamente o por terceros mediante revisiones de arquitectura, análisis de código, pruebas de seguridad y validación de configuraciones, antes de su puesta en producción y ante cambios significativos. Evidencia: informes de pruebas, resultados de revisión, evidencias de configuración y actas de aceptación.
- Verificar la interoperabilidad y portabilidad de los mecanismos criptográficos mediante pruebas de compatibilidad, validación de estándares, procedimientos de recuperación y pruebas de migración, antes de su adopción y cuando se incorporen nuevas tecnologías. Evidencia: resultados de pruebas, documentación técnica y registros de compatibilidad.
- Administrar las llaves criptográficas mediante generación, distribución, almacenamiento seguro, rotación, renovación, respaldo, revocación y destrucción controlada, aplicando controles diferenciados según su criticidad y revisando periódicamente su vigencia. Evidencia: inventario de llaves, registros de ciclo de vida, certificados, logs y actas de destrucción.

- Aplicar la segregación de funciones en la gestión criptográfica mediante roles diferenciados para solicitud, aprobación, administración, custodia y uso de llaves, manteniendo matrices de permisos y revisándolas periódicamente. Evidencia: matriz de roles, registros de asignación, autorizaciones y reportes de revisión.
- Implementar únicamente soluciones y prácticas criptográficas autorizadas mediante un catálogo institucional de algoritmos, protocolos, herramientas, certificados y casos de uso aprobados, actualizándolo cuando cambien los estándares, riesgos o tecnologías disponibles. Evidencia: catálogo criptográfico, lineamientos, registros de actualización y aprobaciones.
- Gestionar certificados de clave pública mediante procedimientos de solicitud, validación, emisión, renovación, revocación y almacenamiento seguro, verificando su vigencia y estado antes de utilizarlos en servicios institucionales. Evidencia: certificados, registros de emisión/renovación, listas de revocación y reportes de vigencia.
- Gestionar la distribución, recuperación y destrucción de claves mediante procedimientos documentados de custodia, respaldo, recuperación ante pérdida o daño, revocación y eliminación segura, aplicándolos cuando ocurra una contingencia o finalice el ciclo de vida de la clave. Evidencia: registros de custodia, solicitudes de recuperación, respaldos, revocaciones y certificados de destrucción.
- Proteger los procesos de cargue automático de archivos provenientes de terceros mediante autenticación basada en certificados, infraestructura de llave pública o mecanismos equivalentes, verificando la identidad del origen y la integridad de los archivos antes de procesarlos. Evidencia: certificados, configuraciones, registros de autenticación y validaciones de integridad.

- Restringir la incorporación de hardware y software con funciones criptográficas no autorizadas mediante evaluación técnica, revisión de especificaciones, catálogo de tecnologías permitidas y controles de adquisición, aplicando la validación antes de su incorporación al ambiente institucional. Evidencia: evaluaciones técnicas, fichas de producto, aprobaciones y registros de adquisición.
- Regular el uso de criptografía mediante un esquema institucional que establezca algoritmos, protocolos, mecanismos, longitudes de clave y técnicas permitidas, basado en estándares nacionales e internacionales vigentes y revisado periódicamente. Evidencia: esquema criptográfico, matriz de algoritmos autorizados y registros de revisión.
- Aplicar algoritmos y protocolos criptográficos autorizados mediante configuraciones técnicas alineadas con los estándares institucionales, evitando algoritmos obsoletos o inseguros y verificando su utilización mediante análisis de configuración y pruebas técnicas. Evidencia: configuraciones, resultados de escaneo, informes de seguridad y registros de actualización.
- Aplicar tecnologías criptográficas para proteger transacciones electrónicas mediante cifrado, firma digital, firma electrónica, certificados y mecanismos de validación, de acuerdo con la criticidad de la transacción y los requisitos de autenticidad, integridad y no repudio. Evidencia: registros de transacciones, certificados, firmas y resultados de validación.
- Aplicar controles criptográficos en soluciones basadas en Blockchain, cuando sean adoptadas, mediante algoritmos, mecanismos de consenso, firmas, funciones hash y controles de identidad alineados con estándares técnicos y guías aplicables al sector público colombiano, verificando su funcionamiento mediante pruebas de seguridad. Evidencia: arquitectura

técnica, configuraciones, resultados de pruebas y documentación de seguridad.

Funcionarios y terceros

- Notificar la necesidad de cifrado de información mediante los canales institucionales establecidos, indicando la clasificación, tipo de información, medio de almacenamiento o transmisión y necesidad de protección, antes de realizar el tratamiento de información reservada, clasificada o de carácter personal. Evidencia: solicitud registrada, clasificación de información y respuesta de atención.
- Solicitar la aplicación de controles criptográficos sobre bases de datos mediante requerimientos formales que identifiquen la información a proteger, sistema, base de datos, nivel de sensibilidad y necesidad de acceso, antes de implementar o modificar el mecanismo de protección. Evidencia: solicitud, análisis técnico, autorización y registro de implementación.
- Aplicar los lineamientos criptográficos institucionales mediante las herramientas, algoritmos, protocolos y mecanismos autorizados, verificando su utilización durante las actividades de almacenamiento, procesamiento y transmisión de información protegida. Evidencia: configuraciones, registros de uso, resultados de validación y reportes de cumplimiento.
- Cifrar y generar un valor hash antes de transmitir información protegida por correo institucional mediante las herramientas criptográficas autorizadas, aplicando el cifrado y cálculo de integridad antes del envío y verificando el valor hash cuando se reciba la información. Evidencia: archivo cifrado, registro o valor hash, correo de envío y evidencia de validación.

- Proteger las claves criptográficas mediante almacenamiento en mecanismos seguros, control de acceso y restricción de uso a personas autorizadas, manteniendo una copia de recuperación cuando el procedimiento institucional lo permita y verificando periódicamente su disponibilidad. Evidencia: registros de custodia, controles de acceso, inventario de claves y pruebas de recuperación.
- Aplicar las condiciones de cifrado para el correo electrónico mediante los mecanismos definidos para información pública reservada y clasificada, verificando antes del envío que el mensaje y sus archivos adjuntos cumplen las condiciones de protección establecidas. Evidencia: mensajes enviados, registros de cifrado y resultados de verificación.
- Proteger la información pública reservada y clasificada y los datos personales mediante cifrado durante el almacenamiento y transmisión, controles de acceso y mecanismos de integridad, aplicando las medidas durante todo el ciclo de vida de la información y verificando periódicamente su cumplimiento. Evidencia: configuraciones de cifrado, registros de acceso, reportes de cumplimiento y resultados de auditoría.

8.15. Componente Política de Seguridad de Aplicaciones

8.15.1. Uso de programas privilegiados de utilidad: Control Asociado en el MSPI: 8.18

Garantizar que el uso de programas de utilidad no perjudique los controles de sistema y de las aplicaciones para seguridad de la información. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Restringir la instalación de software y los cambios de configuración del sistema mediante políticas de grupo (GPO) aplicadas desde el

controlador de dominio, control de privilegios administrativos y listas de software autorizado, verificando su aplicación en los equipos vinculados al dominio y actualizándolas cuando se modifiquen los requerimientos de seguridad. Evidencia: GPO configuradas, políticas de seguridad, reportes de cumplimiento y registros de cambios.

- Eliminar los privilegios de administrador de los usuarios finales mediante perfiles estándar, control de privilegios y administración centralizada de identidades, manteniendo únicamente las cuentas administrativas estrictamente necesarias y revisando periódicamente los privilegios asignados. Evidencia: inventario de cuentas privilegiadas, matriz de permisos, reportes de cumplimiento y registros de revisión.
- Controlar el uso de programas utilitarios mediante un procedimiento de solicitud, justificación, evaluación de riesgo, autorización, instalación y revocación, aplicándolo cada vez que un funcionario o tercero requiera utilizar una herramienta con capacidades administrativas o de configuración. Evidencia: solicitudes, autorizaciones, evaluación de riesgo, inventario de utilitarios y registros de instalación/desinstalación.
- Mantener actualizado el inventario de programas utilitarios autorizados mediante un registro centralizado que incluya nombre, versión, fabricante, propósito, usuarios autorizados, activos donde se encuentra instalado y vigencia de la autorización, actualizándolo ante cada alta, modificación o revocación. Evidencia: inventario de utilitarios, historial de cambios y registros de autorización.
- Restringir las herramientas de administración licenciadas mediante controles de acceso basados en roles, cuentas administrativas individuales y permisos mínimos, permitiendo su ejecución únicamente a usuarios previamente autorizados y revisando periódicamente las asignaciones. Evidencia: matriz de accesos, configuración de permisos,

registros de ejecución y reportes de revisión.

- Aplicar las políticas de dominio que bloquean la instalación de software y modificaciones no autorizadas mediante GPO, control de aplicaciones, restricciones de privilegios y mecanismos de administración centralizada, verificando periódicamente su aplicación y generando alertas ante intentos de incumplimiento. Evidencia: GPO, reportes de cumplimiento, logs de eventos y alertas de seguridad.
- Verificar que los usuarios finales no dispongan de privilegios administrativos mediante revisiones periódicas de grupos locales y del dominio, herramientas de gestión de endpoints y comparación contra la matriz de accesos autorizados, realizando la corrección inmediata de privilegios no justificados. Evidencia: reportes de grupos administrativos, inventario de cuentas, tickets de remediación y resultados de revisión.
- Bloquear automáticamente las sesiones después de cinco minutos de inactividad mediante políticas de bloqueo de pantalla aplicadas desde el sistema operativo o GPO, manteniendo la sesión de las aplicaciones y conexiones de red cuando técnicamente corresponda y verificando periódicamente el comportamiento de la política. Evidencia: configuración de GPO, políticas de seguridad, resultados de pruebas y reportes de cumplimiento.
- Suspender o bloquear las estaciones de trabajo después de períodos superiores a dos horas sin actividad mediante políticas de administración de energía, bloqueo o suspensión configuradas centralmente, aplicándolas cuando no exista actividad durante el periodo definido y exceptuando únicamente los equipos con justificación técnica autorizada. Evidencia: configuraciones de energía, políticas aplicadas, reportes de cumplimiento y registros de excepciones.

- Limitar el número de usuarios autorizados para utilizar programas utilitarios mediante grupos de seguridad, roles específicos, cuentas individuales y principio de mínimo privilegio, revisando periódicamente la pertenencia a dichos grupos y retirando los accesos que ya no sean necesarios. Evidencia: grupos de seguridad, matriz de accesos, inventario de usuarios autorizados y reportes de revisión.
- Separar lógicamente los programas utilitarios del software de aplicación mediante permisos diferenciados, repositorios controlados, rutas o ambientes separados y mecanismos de control de ejecución, evitando que los usuarios estándar puedan modificar, reemplazar o ejecutar herramientas administrativas no autorizadas. Evidencia: configuración de permisos, políticas de ejecución, inventario de software y resultados de pruebas.

8.15.2. Ciclo de vida de desarrollo seguro

Control Asociado en el MSPI: 8.25

Garantizar que seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de "software" y sistemas. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Controlar la transferencia de software desde desarrollo hacia producción mediante un procedimiento formal de gestión de versiones y cambios que incluya revisión de código, pruebas, aprobación, control de versiones, criterios de aceptación y autorización de paso a producción, aplicándolo a cada liberación y a los desarrollos realizados internamente o por terceros. Evidencia: solicitudes de cambio, versiones liberadas, resultados de pruebas, aprobaciones y registros de despliegue.

- Aplicar metodologías de desarrollo seguro mediante la incorporación de requisitos de seguridad desde la definición de requerimientos, análisis de riesgos, revisión de código, pruebas de seguridad, análisis de vulnerabilidades y prácticas de codificación segura, utilizándolas durante todas las etapas del ciclo de desarrollo. Evidencia: metodología adoptada, requisitos de seguridad, listas de verificación, resultados de análisis y pruebas.
- Mantener separados los ambientes de desarrollo, pruebas, integración y producción mediante segmentación de redes, controles de acceso diferenciados, cuentas independientes, repositorios separados y reglas de firewall, evitando accesos o intercambios no autorizados entre ambientes y verificando periódicamente el aislamiento. Evidencia: diagramas de arquitectura, configuraciones de red, matrices de acceso, reglas de firewall y resultados de pruebas de aislamiento.
- Aplicar los lineamientos y controles de desarrollo seguro mediante listas de verificación, controles técnicos, revisiones de cumplimiento y puntos de control durante el ciclo de desarrollo, verificando su aplicación antes de aprobar cada liberación hacia producción. Evidencia: listas de verificación, informes de revisión, registros de cumplimiento y aprobaciones de liberación.
- Mantener actualizada la plataforma tecnológica y las herramientas de desarrollo mediante gestión de parches, actualizaciones controladas, inventario de versiones y monitoreo de vulnerabilidades, verificando periódicamente que los componentes utilicen versiones soportadas y aprobadas y aplicando las actualizaciones de seguridad según su criticidad. Evidencia: inventario de versiones, reportes de parcheo, resultados de escaneo de vulnerabilidades y registros de actualización.
- Validar las herramientas utilizadas para desarrollar o adquirir sistemas

de información mediante revisión de licenciamiento, soporte del fabricante, procedencia, reputación y compatibilidad técnica, realizando la validación antes de su incorporación al ciclo de desarrollo o adquisición. Evidencia: licencias, contratos, fichas técnicas, registros de validación y aprobaciones.

- Aplicar los requisitos de seguridad y privacidad durante todo el ciclo de desarrollo mediante puntos de control en las fases de análisis, diseño, desarrollo, pruebas, implementación, mantenimiento y retiro, verificando el cumplimiento del manual de seguridad, requisitos legales y lineamientos institucionales antes de cada liberación significativa. Evidencia: listas de verificación, matrices de requisitos, resultados de revisiones, informes de pruebas y actas de aprobación.
- Proteger el código fuente mediante repositorios institucionales con autenticación individual, control de acceso basado en roles, mínimo privilegio, control de versiones y registro de actividades, restringiendo la descarga, modificación o eliminación a usuarios autorizados y revisando periódicamente los permisos. Evidencia: matriz de accesos, logs del repositorio, historial de versiones, registros de cambios y reportes de revisión.
- Proteger la información utilizada en ambientes de desarrollo y pruebas mediante enmascaramiento, anonimización o generación de datos sintéticos, aplicándolo antes de trasladar información desde producción y verificando que no se incorporen datos personales reales o información confidencial sin autorización y controles específicos. Evidencia: procedimientos de enmascaramiento/anonimización, resultados de validación, registros de transferencia y muestras de datos de prueba.
- Controlar la transferencia de información entre ambientes mediante mecanismos autorizados de transferencia, permisos diferenciados,

trazabilidad y validación previa de la clasificación de la información, aplicando controles adicionales cuando excepcionalmente se requiera utilizar información real en pruebas. Evidencia: solicitudes de transferencia, autorizaciones, registros de acceso, logs de transferencia y resultados de revisión.

- Verificar la correcta separación y funcionamiento de los ambientes de desarrollo, pruebas, integración y producción mediante pruebas de conectividad, revisión de reglas de firewall, validación de cuentas y permisos, análisis de rutas de comunicación y comprobación de las configuraciones de cada ambiente, ejecutándolas durante la implementación y después de cambios relevantes. Evidencia: resultados de pruebas, diagramas actualizados, configuraciones, matrices de acceso y reportes de validación.

8.15.3. Requisitos de seguridad de las aplicaciones

Control Asociado en el MSPI: 8.26

Garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Identificar y especificar los requisitos de seguridad de cada aplicación mediante análisis de riesgos, clasificación de la información, identificación de amenazas, requisitos legales y necesidades del proceso de negocio, realizándolo durante el levantamiento de requerimientos y actualizándolo ante cambios relevantes en la aplicación. Evidencia: matriz de requisitos de seguridad, análisis de riesgos, historias de usuario/requisitos y aprobaciones.
- Determinar el nivel de confianza requerido para la identidad de los

usuarios mediante análisis de criticidad de la aplicación, sensibilidad de la información y riesgo de acceso, definiendo los mecanismos de autenticación y validación de identidad antes de iniciar el desarrollo. Evidencia: matriz de autenticación, análisis de riesgos y especificaciones de seguridad.

- Clasificar la información procesada por cada aplicación mediante consulta del inventario de activos y aplicación de los criterios institucionales de clasificación, documentando el nivel de clasificación antes de definir los controles técnicos. Evidencia: matriz de clasificación, inventario de información y requisitos de seguridad.
- Implementar segregación de acceso a datos y funcionalidades mediante roles, perfiles, permisos, mínimo privilegio y segregación de funciones, aplicándolos desde el diseño y verificándolos mediante pruebas de autorización antes de la puesta en producción. Evidencia: matriz de roles, configuración de permisos, casos de prueba y resultados de validación.
- Incorporar mecanismos de resiliencia frente a ataques e interrupciones mediante validaciones de entrada, límites de recursos, manejo seguro de errores, protección contra inyección, desbordamiento, denegación de servicio y otras vulnerabilidades identificadas, verificándolos durante las pruebas de seguridad. Evidencia: especificaciones técnicas, resultados de SAST/DAST, pruebas de penetración y registros de remediación.
- Incorporar requisitos legales, regulatorios y contractuales mediante matrices de cumplimiento que identifiquen las obligaciones aplicables según el lugar donde se genere, procese, transmita o almacene la información, validándolas durante el diseño y antes de la liberación. Evidencia: matriz legal, requisitos de cumplimiento, revisiones y aprobaciones.

- Aplicar requisitos de privacidad mediante identificación de titulares, finalidades, tipos de datos tratados, minimización, controles de acceso, conservación y mecanismos de protección, incorporándolos al diseño de la aplicación cuando se procesen datos personales. Evidencia: análisis de privacidad, matriz de datos, requisitos funcionales y pruebas de cumplimiento.
- Proteger la información confidencial mediante controles de acceso, cifrado, segregación, enmascaramiento y monitoreo, aplicándolos durante el procesamiento, almacenamiento y transmisión según la clasificación de la información. Evidencia: arquitectura de seguridad, configuraciones, pruebas de acceso y evidencias de cifrado.
- Proteger los datos en proceso, tránsito y reposo mediante controles de memoria y aplicación, protocolos seguros, cifrado de bases de datos, discos y medios de almacenamiento, verificando su configuración durante las pruebas técnicas y revisiones de seguridad. Evidencia: arquitectura, configuraciones criptográficas, certificados y resultados de pruebas.
- Cifrar las comunicaciones entre las partes involucradas mediante protocolos seguros, certificados digitales y algoritmos criptográficos aprobados, validando la configuración antes de poner el servicio en producción y ante modificaciones de las interfaces. Evidencia: configuración TLS/HTTPS/VPN, certificados, pruebas de cifrado y reportes de vulnerabilidades.
- Validar las entradas de las aplicaciones mediante listas de validación que comprueben fuente, tipo, formato, rango, longitud, caracteres permitidos y datos inesperados, ejecutando las validaciones antes de procesar cualquier entrada y verificándolas mediante pruebas de seguridad. Evidencia: código fuente, listas de validación, casos de

prueba y resultados de SAST/DAST.

- Implementar controles automatizados para operaciones críticas mediante límites de aprobación, doble validación, segregación de funciones y reglas de negocio, activándolos cuando la transacción supere los umbrales o condiciones definidos. Evidencia: reglas configuradas, matriz de autorizaciones, logs de aprobación y casos de prueba.
- Controlar las salidas de información mediante perfiles de autorización, filtros de datos, clasificación y reglas de visualización o exportación, restringiendo el acceso de acuerdo con el rol y necesidad funcional. Evidencia: matriz de permisos, reglas de salida, registros de acceso y pruebas de autorización.
- Restringir el contenido de campos de texto libre mediante validaciones, expresiones de control, clasificación de datos y mecanismos de detección de información sensible, evitando el almacenamiento no controlado de datos personales o confidenciales y revisando los campos durante las pruebas de seguridad. Evidencia: especificaciones, reglas de validación, resultados de pruebas y reportes de hallazgos.
- Implementar trazabilidad y no repudio de las transacciones mediante identificadores únicos, sellos de tiempo, registros de auditoría, firmas electrónicas o digitales cuando corresponda, manteniendo la trazabilidad durante todo el ciclo de la transacción. Evidencia: logs de transacciones, registros de auditoría, firmas y reportes de trazabilidad.
- Integrar los requisitos derivados de otros controles de seguridad mediante interfaces para SIEM, monitoreo, auditoría, DLP, gestión de vulnerabilidades y detección de eventos, definiéndolos durante la arquitectura y verificando su funcionamiento antes de la puesta en producción. Evidencia: diagramas de integración, configuraciones, logs recibidos y resultados de pruebas.

- Gestionar los mensajes de error de forma segura mediante mensajes controlados que no expongan credenciales, rutas, código fuente, consultas, configuraciones ni información sensible, registrando el detalle técnico únicamente en los logs protegidos. Evidencia: casos de prueba, configuración de errores, ejemplos de mensajes y registros de aplicación.
- Identificar los requisitos de seguridad de servicios y transacciones mediante análisis de interfaces, APIs, integraciones, flujos de información, autenticación y riesgos asociados, aplicándolos tanto a desarrollos internos como subcontratados antes de su implementación. Evidencia: especificaciones de APIs, diagramas de integración, matriz de requisitos y análisis de riesgos.
- Incorporar requisitos de desarrollo seguro en los contratos de terceros mediante cláusulas técnicas que incluyan seguridad desde el diseño, protección de código, pruebas, gestión de vulnerabilidades, privacidad, control de accesos y entrega de evidencias, verificando su cumplimiento durante la ejecución contractual. Evidencia: contrato, anexos técnicos, listas de verificación, informes de pruebas y actas de aceptación.
- Aplicar prácticas reconocidas de desarrollo seguro mediante OWASP, Secure Software Development Lifecycle y referencias técnicas como CWE, CERT Secure Coding, CIS Controls, WASC y demás estándares institucionalmente adoptados, utilizándolas durante diseño, codificación, pruebas y liberación. Evidencia: metodología de desarrollo, listas de verificación, resultados de análisis y reportes de cumplimiento.
- Implementar controles de validación de entradas mediante listas de comprobación y validaciones automáticas de fuentes, tipos, rangos, longitudes, formatos, caracteres peligrosos y valores inesperados, incorporándolos en cada componente que reciba información externa.

Evidencia: código fuente, pruebas unitarias, SAST/DAST y resultados de validación.

- Sanear las salidas de datos no confiables mediante consultas parametrizadas, codificación contextual, APIs seguras y mecanismos de escape, aplicándolos antes de enviar datos a SQL, XML, LDAP, comandos del sistema operativo u otros intérpretes y verificándolos mediante pruebas de seguridad. Evidencia: código fuente, resultados de SAST/DAST, pruebas de inyección y reportes de remediación.
- Proteger la autenticación y las credenciales mediante autenticación centralizada, protocolos estándar, almacenamiento seguro mediante funciones criptográficas apropiadas, políticas de bloqueo y recuperación segura, evitando el envío de contraseñas por correo y verificando estos controles durante las pruebas de seguridad. Evidencia: configuración de autenticación, resultados de pruebas, políticas de contraseñas y registros de eventos.
- Gestionar las sesiones de las aplicaciones mediante identificadores de sesión aleatorios, expiración, invalidación, regeneración posterior a la autenticación y controles contra sesiones concurrentes cuando el riesgo lo requiera, verificando su comportamiento mediante pruebas de seguridad antes de la liberación. Evidencia: configuración de sesión, código, casos de prueba, resultados de DAST y reportes de seguridad.
- Implementar controles de acceso en las aplicaciones mediante autorización del lado servidor, RBAC/ABAC, validación de URL y funciones protegidas, protección contra referencias directas a objetos y restricciones sobre servicios, aplicándolos a cada recurso y función protegida y verificándolos mediante pruebas negativas de autorización. Evidencia: matriz de permisos, configuración de roles, resultados de pruebas y reportes de vulnerabilidades.

- Limitar la cantidad de transacciones realizadas por usuarios o dispositivos mediante controles de tasa, límites de frecuencia, cuotas y mecanismos de protección contra abuso, aplicándolos según la criticidad del servicio y verificándolos mediante pruebas de carga y seguridad. Evidencia: configuración de rate limiting, métricas, logs y resultados de pruebas.
- Configurar registros de seguridad de las aplicaciones mediante logs de fallas de validación, intentos de autenticación, fallas de control de acceso y eventos asociados a intentos de evasión de controles, centralizándolos cuando corresponda y revisando periódicamente su generación e integridad. Evidencia: configuración de logging, registros de aplicación, integración con SIEM y resultados de pruebas.
- Aplicar el principio de mínimo privilegio sobre los datos y funcionalidades mediante roles, perfiles, permisos específicos y segregación de funciones, otorgando únicamente los accesos requeridos para cada actividad y revisándolos periódicamente o ante cambios de rol. Evidencia: matriz de accesos, registros de autorización, reportes de revisión y logs.
- Eliminar aplicaciones, componentes y documentación innecesarios mediante inventarios de software, revisión de dependencias, análisis de componentes y depuración controlada de documentación técnica, realizando la eliminación antes de la puesta en producción y durante las revisiones periódicas de mantenimiento. Evidencia: inventario actualizado, registros de eliminación, resultados de análisis y evidencias de revisión.

8.15.4. Principios de ingeniería y arquitectura de sistemas seguros

Control Asociado en el MSPI: 8.27

Garantizar que los sistemas de información se diseñan, implementan y operan de forma segura dentro del ciclo de vida de desarrollo. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Implementar y mantener lineamientos y criterios de desarrollo seguro mediante estándares, guías, metodologías y procedimientos que incorporen controles de seguridad desde el diseño, construcción, mantenimiento y ajuste de los sistemas de información y software. Actualizar estos instrumentos cuando se incorporen nuevas tecnologías, cambios relevantes o requisitos de seguridad. Evidencia: lineamientos, guías, procedimientos, registros de actualización y versiones aprobadas.
- Incorporar controles de seguridad y privacidad en las capas de arquitectura de negocio, datos, aplicaciones y tecnología mediante análisis de riesgos, clasificación de la información, requisitos de protección de datos personales y principios de privacidad desde el diseño, de acuerdo con la Ley 1581 de 2012 y demás normativa aplicable. Aplicar estos controles durante el diseño y modificación de los sistemas. Evidencia: arquitecturas aprobadas, matrices de requisitos de seguridad y privacidad, análisis de riesgos y registros de revisión.
- Analizar patrones y técnicas de ataque conocidas mediante el uso de fuentes de inteligencia de amenazas, vulnerabilidades identificadas, incidentes registrados y marcos de desarrollo seguro, incorporando los controles preventivos y de mitigación correspondientes durante la construcción o modificación de los sistemas. Realizar la revisión antes de la puesta en producción y cuando se identifiquen nuevas amenazas

relevantes. Evidencia: análisis de amenazas, matrices de controles, registros de vulnerabilidades y resultados de pruebas de seguridad.

- Revisar y actualizar los lineamientos, principios y procedimientos de desarrollo seguro mediante evaluaciones periódicas, resultados de auditorías, incidentes, vulnerabilidades, cambios tecnológicos y nuevas amenazas. Realizar la revisión al menos una vez al año o cuando se presenten cambios significativos, aplicando el control de versiones establecido en el Sistema de Gestión Documental. Evidencia: documentos versionados, registros de revisión, aprobaciones, historial de cambios y actas.
- Verificar la aplicación del ciclo de desarrollo seguro en los sistemas construidos o mantenidos por terceros mediante requisitos contractuales, listas de verificación, revisiones de entregables, análisis de código, pruebas de seguridad y validaciones previas a la puesta en producción. Aplicar la verificación durante las etapas definidas del ciclo de desarrollo y antes de aceptar los entregables. Evidencia: contratos, listas de verificación, informes de revisión, resultados de pruebas, hallazgos y actas de aceptación.
- Implementar capacidades de prevención, detección y respuesta frente a eventos de seguridad mediante controles de autenticación, autorización, validación de entradas, protección de datos, registro de eventos, monitoreo, alertamiento y mecanismos de respuesta integrados en los sistemas de información. Validar estos controles durante las pruebas de seguridad y antes de la puesta en producción, y monitorearlos durante la operación. Evidencia: configuraciones, registros de eventos, alertas, resultados de pruebas y reportes de monitoreo.
- Aplicar los principios de confianza cero y desarrollo seguro mediante controles de seguridad por diseño, defensa en profundidad, seguridad

por defecto, denegación predeterminada, fallo seguro, validación de entradas externas, seguridad en la implementación, asunción de compromiso, mínimo privilegio, facilidad de uso y administración y funcionalidad mínima. Verificar su aplicación durante el diseño, desarrollo, pruebas y cambios relevantes del sistema. Evidencia: diseños de arquitectura, matrices de controles, configuraciones, resultados de pruebas de seguridad y registros de revisión.

- Transacciones mediante redes de telecomunicaciones
- Verificar la incorporación de controles de seguridad en las transacciones electrónicas mediante requisitos técnicos y listas de verificación que contemplen autenticación, criptografía, confidencialidad, privacidad, protección de las comunicaciones, protocolos seguros y almacenamiento protegido. Aplicar la verificación durante el diseño, integración, pruebas y modificación de los servicios transaccionales. Evidencia: requisitos de seguridad, listas de verificación, diseños técnicos, resultados de pruebas y registros de aprobación.
- Aplicar mecanismos criptográficos en las transacciones mediante algoritmos, protocolos y certificados aprobados institucionalmente, protegiendo la información intercambiada entre las partes durante su transmisión y procesamiento. Verificar su configuración y vigencia antes de la puesta en producción y durante revisiones periódicas. Evidencia: configuraciones criptográficas, certificados, resultados de pruebas y reportes de revisión.
- Validar la información de autenticación mediante mecanismos de autenticación robusta, validación de credenciales, controles de integridad y protección contra reutilización, interceptación o modificación de las credenciales de las partes involucradas. Aplicar estos controles en cada transacción que requiera autenticación. Evidencia:

registros de autenticación, configuraciones, políticas de acceso y resultados de pruebas.

- Proteger la confidencialidad y privacidad de las transacciones mediante cifrado, controles de acceso, minimización de datos y aplicación de las medidas de protección definidas para la información tratada. Aplicar estos controles durante todo el ciclo de la transacción y verificar su efectividad en las pruebas de seguridad. Evidencia: configuraciones, registros de acceso, resultados de pruebas y reportes de validación.
- Cifrar las comunicaciones entre las partes involucradas mediante protocolos seguros y mecanismos criptográficos aprobados, evitando el envío de información protegida mediante canales no cifrados. Verificar el cifrado en cada integración o modificación de los servicios transaccionales y mediante revisiones periódicas. Evidencia: configuraciones de TLS/SSL u otros protocolos aprobados, certificados, pruebas de conexión segura y resultados de análisis técnicos.
- Utilizar protocolos seguros de comunicación mediante configuraciones basadas en estándares institucionales y eliminación o deshabilitación de protocolos, algoritmos y versiones obsoletas o vulnerables. Revisar la configuración durante la implementación, los cambios tecnológicos y las evaluaciones periódicas de seguridad. Evidencia: configuraciones, informes de vulnerabilidades, resultados de pruebas y registros de cambios.
- Proteger el almacenamiento de la información transaccional mediante bases de datos, repositorios o servicios ubicados en redes internas o segmentos protegidos, aplicando controles de acceso, cifrado cuando corresponda y restricciones de exposición directa a Internet. Verificar la configuración antes de la puesta en producción y durante las revisiones de seguridad. Evidencia: diagramas de arquitectura, reglas de firewall,

configuraciones de acceso, resultados de análisis de exposición y registros de revisión.

- Integrar la seguridad en la gestión de certificados y firmas digitales de extremo a extremo mediante controles para la solicitud, validación, emisión, instalación, renovación, almacenamiento, uso, revocación y eliminación de certificados y claves asociadas. Aplicar los controles durante todo el ciclo de vida y verificar periódicamente su vigencia y configuración. Evidencia: inventario de certificados, registros de emisión y renovación, configuraciones, solicitudes de revocación, registros de auditoría y resultados de verificaciones.

8.15.5. Codificación segura:

Control Asociado en el MSPI: 8.28

Garantizar que el "software" se escribe de forma segura, reduciendo así el número de posibles vulnerabilidades de seguridad de la información en el "software". Por lo tanto, se desarrollarán las siguientes actividades:

Seguridad de la Información

- Monitorear y actualizar la base de conocimiento sobre amenazas, vulnerabilidades y técnicas de explotación mediante fuentes de inteligencia de amenazas, boletines de fabricantes, bases de vulnerabilidades, resultados de análisis de seguridad e incidentes identificados. Realizar el seguimiento de manera continua y actualizar la información cuando se identifiquen nuevas vulnerabilidades o amenazas relevantes, utilizándola para orientar la aplicación de principios de codificación segura y fortalecer las prácticas de desarrollo. Evidencia: registros de monitoreo, boletines analizados, base de conocimiento actualizada, reportes de vulnerabilidades y recomendaciones de

seguridad.

La SIDT

- Implementar y mantener prácticas de codificación segura durante las etapas de planificación, desarrollo, revisión, mantenimiento y modificación del software mediante estándares, guías, listas de verificación y controles técnicos integrados al ciclo de desarrollo. Aplicarlas en cada nuevo desarrollo, cambio o mantenimiento significativo. Evidencia: estándares de codificación, listas de verificación, revisiones de código, resultados de pruebas y registros de cambios.
- Aplicar controles de codificación segura mediante validación de entradas, gestión segura de errores, control de autenticación y autorización, protección de datos, gestión de sesiones, prevención de vulnerabilidades conocidas y revisión de código. Verificar su aplicación durante el desarrollo y antes de la puesta en producción. Evidencia: código revisado, resultados de análisis SAST/DAST, pruebas de seguridad, hallazgos y registros de remediación.
- Implementar líneas base de desarrollo seguro mediante configuraciones estandarizadas para herramientas, lenguajes, frameworks, librerías, componentes de terceros y software de código abierto, incorporando requisitos de seguridad, versiones soportadas y controles mínimos. Aplicarlas antes de iniciar el desarrollo y revisarlas cuando se presenten cambios tecnológicos, vulnerabilidades o actualizaciones de componentes. Evidencia: líneas base aprobadas, configuraciones, inventario de componentes, versiones utilizadas y registros de revisión.

- Requisitos previos para la codificación segura

- Configurar las herramientas de desarrollo mediante IDE, compiladores, analizadores de código, repositorios y complementos que incorporen validaciones, alertas y controles de seguridad durante la construcción del software. Validar la configuración antes de iniciar los desarrollos y ante cambios relevantes en las herramientas. Evidencia: configuraciones de herramientas, listas de verificación y resultados de validación.
- Aplicar las recomendaciones de seguridad de los fabricantes mediante la consulta de documentación técnica, guías de configuración segura, avisos de vulnerabilidades y buenas prácticas para las herramientas de desarrollo y entornos de ejecución. Revisarlas durante la implementación, actualización o modificación de las plataformas. Evidencia: guías consultadas, configuraciones aplicadas, registros de actualización y resultados de revisión.
- Mantener actualizadas las herramientas de desarrollo mediante procesos de gestión de versiones y actualización de IDE, compiladores, intérpretes, librerías y demás componentes utilizados en el desarrollo. Realizar las actualizaciones de acuerdo con la criticidad de las vulnerabilidades, soporte del fabricante y resultados del análisis de riesgos. Evidencia: inventario de versiones, registros de actualización, reportes de vulnerabilidades y evidencias de pruebas de compatibilidad.
- Validar las competencias en codificación segura mediante criterios técnicos definidos para los perfiles de desarrollo, evaluación de conocimientos y formación en prácticas de desarrollo seguro. Realizar la validación durante la incorporación al equipo y actualizar los conocimientos periódicamente o ante cambios relevantes en las tecnologías y amenazas. Evidencia: registros de capacitación, evaluaciones, certificaciones y planes de formación.
- Incorporar seguridad en el diseño y arquitectura mediante análisis de

amenazas, requisitos de seguridad, modelado de riesgos, segregación de componentes, mínimo privilegio y principios de seguridad por diseño. Aplicar estos controles antes de iniciar la construcción y revisarlos ante cambios significativos de arquitectura. Evidencia: arquitecturas aprobadas, modelos de amenazas, requisitos de seguridad y matrices de riesgos.

- Aplicar normas de codificación segura mediante estándares institucionales y buenas prácticas reconocidas para los lenguajes y tecnologías utilizados, incluyendo controles para prevenir vulnerabilidades de código conocidas. Verificar su cumplimiento mediante revisiones de código y herramientas automatizadas durante el ciclo de desarrollo. Evidencia: estándares de codificación, listas de verificación, informes SAST y resultados de revisión de código.
- Utilizar ambientes controlados para el desarrollo mediante la separación de los entornos de desarrollo, pruebas y producción, controles de acceso, autenticación individual, protección de repositorios y restricción del uso de información productiva. Mantener la segregación durante todo el ciclo de desarrollo. Evidencia: diagramas de ambientes, configuraciones de acceso, registros de autenticación y controles de segregación.
- Capacitar en codificación segura mediante sesiones prácticas, talleres, análisis de vulnerabilidades, ejercicios sobre errores frecuentes y divulgación de nuevas técnicas de ataque y mecanismos de prevención. Realizar la capacitación periódicamente y ante la incorporación de nuevas tecnologías o amenazas relevantes. Evidencia: plan y registros de capacitación, material utilizado, asistencia, evaluaciones y resultados de ejercicios.
- Prevenir el uso de técnicas inseguras mediante estándares de desarrollo, revisión de código, análisis automatizado y controles que identifiquen

prácticas vulnerables durante las fases de diseño, codificación, pruebas y mantenimiento. Corregir los hallazgos antes de la puesta en producción o conforme a los plazos definidos según su criticidad. Evidencia: reportes de análisis, hallazgos, registros de corrección y resultados de validación.

- Analizar vulnerabilidades del código mediante herramientas SAST, DAST, análisis de dependencias, revisión manual y pruebas especializadas para sistemas críticos y desarrollos institucionales. Realizar los análisis durante el ciclo de desarrollo, antes de la puesta en producción y ante cambios significativos. Evidencia: informes de análisis, resultados de pruebas, inventario de vulnerabilidades y registros de remediación.
- Identificar y analizar errores frecuentes de codificación mediante la revisión de vulnerabilidades detectadas, incidentes, resultados de pruebas y patrones de fallas recurrentes, consolidándolos en una base de conocimiento para prevenir su repetición. Actualizar el análisis cuando se identifiquen nuevos errores o vulnerabilidades y comunicar las medidas de mitigación al equipo de desarrollo. Evidencia: catálogo de errores, análisis de causas, recomendaciones, registros de divulgación y evidencias de mitigación.
- Gestionar el código fuente mediante control de versiones utilizando repositorios institucionales, identificación individual de desarrolladores, ramas de desarrollo, historial de cambios, revisión de código, control de acceso y mecanismos de recuperación. Aplicar el versionamiento a todo código institucional y registrar cada modificación antes de su integración o despliegue. Evidencia: repositorios, historial de commits, ramas, solicitudes de cambio, revisiones de código y registros de aprobación.
-

8.15.6. Pruebas de seguridad en desarrollo y aceptación

Control Asociado en el MSPI: 8.29

Validar si se cumplen requisitos de seguridad de información cuando las aplicaciones o código se despliegan en entorno de producción. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Definir y documentar el alcance de las pruebas mediante criterios basados en la criticidad, clasificación de la información, arquitectura, complejidad, riesgos y naturaleza del sistema, aplicación o software. Establecer el alcance antes de iniciar cada ciclo de pruebas y ajustarlo cuando se presenten cambios significativos o nuevos riesgos. Evidencia: plan de pruebas, matriz de alcance, análisis de riesgos y registros de aprobación.
- Planificar y ejecutar pruebas durante el ciclo de desarrollo mediante un programa que establezca actividades, escenarios, datos de entrada, condiciones de ejecución, resultados esperados, criterios de aceptación y mecanismos de registro de resultados. Aplicar el programa en las etapas definidas del ciclo de desarrollo y antes de cada puesta en producción. Evidencia: plan de pruebas, casos de prueba, datos de entrada, resultados obtenidos, incidencias y reportes de ejecución.
- Incorporar requisitos de seguridad de la información en los casos de prueba mediante criterios de confidencialidad, integridad, disponibilidad, autenticación, autorización, protección de datos, gestión de sesiones, validación de entradas, trazabilidad y resistencia frente a vulnerabilidades conocidas. Aplicarlos de acuerdo con la criticidad y características del sistema y verificarlos antes de la puesta en producción. Evidencia: matriz de requisitos de seguridad, casos de prueba, resultados y reportes de vulnerabilidades.

- Ejecutar y documentar las pruebas funcionales mediante los formatos institucionales vigentes, validando los requerimientos funcionales y los criterios de aceptación definidos para cada sistema. Completar y aprobar los registros antes de cualquier puesta en producción. Evidencia: formatos de pruebas funcionales diligenciados, resultados, incidencias y certificación de aceptación.
- Ejecutar y certificar las pruebas no funcionales y de seguridad mediante los formatos institucionales establecidos y la consolidación de evidencias técnicas correspondientes a disponibilidad, rendimiento, capacidad, autenticación, autorización, vulnerabilidades y demás controles aplicables. Realizar estas pruebas antes de la puesta en producción y después de cambios significativos que puedan afectar la seguridad. Evidencia: formatos de certificación, informes de pruebas, resultados técnicos, evidencias consolidadas y registros de hallazgos.
- Documentar la aceptación de las pruebas realizadas mediante la revisión de resultados frente a los criterios de aceptación establecidos y el registro formal de conformidad, observaciones o rechazo. Realizar la aceptación antes de autorizar el paso a producción. Evidencia: actas, formatos de aceptación, aprobaciones y registros de observaciones.
- Ejecutar las pruebas de aceptación en un ambiente de staging mediante un entorno segregado de producción que reproduzca las condiciones técnicas relevantes y permita validar funcionalidad, seguridad, integración y comportamiento antes del despliegue. Realizar las pruebas antes de cada puesta en producción y repetirlas cuando existan cambios significativos. Evidencia: resultados de pruebas de staging, registros de despliegue, listas de verificación y evidencias de aceptación.
- Mantener la equivalencia técnica entre los ambientes de prueba y producción mediante configuraciones, versiones, componentes,

servicios, reglas de seguridad y parámetros comparables, conservando la separación lógica y de acceso entre desarrollo, pruebas y producción. Verificar la equivalencia antes de las pruebas de aceptación y ante cambios de infraestructura o configuración. Evidencia: matrices de comparación, configuraciones, diagramas de ambientes, listas de verificación y reportes de validación.

- Implementar pruebas automatizadas mediante herramientas integradas al ciclo de integración y entrega continua (CI/CD), automatizando la ejecución de pruebas funcionales, regresión, integración y validaciones de seguridad según la naturaleza del sistema. Ejecutarlas en cada compilación, cambio de código o despliegue definido en el pipeline. Evidencia: configuración del pipeline, scripts de pruebas, registros de ejecución, resultados y reportes automatizados.
- Detectar y corregir errores en los sistemas mediante pruebas funcionales, de integración, regresión y validaciones automatizadas y manuales en ambientes controlados. Ejecutar las pruebas durante el desarrollo, antes de la puesta en producción y posteriormente cuando se presenten cambios relevantes o incidentes. Evidencia: casos de prueba, registros de errores, tickets de corrección, resultados de regresión y evidencias de cierre.
- Automatizar las pruebas de rendimiento mediante herramientas que permitan medir tiempos de respuesta, concurrencia, utilización de recursos, rendimiento de transacciones y comportamiento bajo diferentes cargas. Ejecutarlas durante las pruebas de aceptación y ante cambios que puedan afectar el desempeño del sistema. Evidencia: scripts de pruebas, métricas de rendimiento, informes de carga, umbrales definidos y resultados de validación.
- Evaluar la capacidad de los sistemas mediante pruebas de carga, estrés,

volumen y concurrencia, estableciendo umbrales de utilización y capacidad máxima esperada para los recursos críticos. Ejecutar escenarios adicionales cuando se alcancen o superen los límites definidos y antes de incrementos significativos de demanda. Evidencia: resultados de pruebas de capacidad, métricas de CPU, memoria, almacenamiento, red y transacciones, umbrales definidos e informes de análisis.

- Integrar pruebas automatizadas de seguridad estática y dinámica mediante herramientas SAST y DAST incorporadas al proceso de compilación, integración y despliegue, identificando vulnerabilidades en el código fuente, componentes y comportamiento de las aplicaciones en ejecución. Ejecutarlas de forma automática en los ciclos definidos del pipeline y antes de autorizar el despliegue a producción. Evidencia: configuración de herramientas SAST/DAST, reportes de vulnerabilidades, registros de ejecución, resultados de remediación y criterios de aprobación.

- Integrar pruebas automatizadas de penetración y validación de seguridad mediante herramientas especializadas y escenarios controlados incorporados al proceso de compilación e implementación, verificando la explotación de vulnerabilidades previamente identificadas y la efectividad de los controles implementados. Ejecutarlas cuando la criticidad, arquitectura o cambios del sistema lo requieran y antes de la puesta en producción cuando sean aplicables. Evidencia: reportes de pruebas de penetración, resultados de explotación controlada, vulnerabilidades identificadas, evidencias de corrección y aprobación de seguridad.
-
-

8.15.7. Desarrollo externo:

Control Asociado en el MSPI: 8.30

Garantizar la aplicación de las medidas de seguridad de la información requeridas por la organización en desarrollo de sistemas subcontratados. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Entregar el modelo de amenazas aprobado al desarrollador externo mediante canales institucionales autorizados y dejando constancia de la versión, alcance y fecha de entrega. Realizar la entrega antes del inicio del desarrollo y actualizarla cuando se modifiquen los riesgos, arquitectura o alcance del proyecto. Evidencia: modelo de amenazas aprobado, registro de entrega, control de versiones y constancia de recepción.
- Incorporar requisitos de desarrollo seguro en los contratos mediante cláusulas que establezcan la aplicación de buenas prácticas de desarrollo, ejecución y entrega de pruebas de seguridad, análisis de vulnerabilidades, gestión de hallazgos y remediación antes de la aceptación del software. Aplicar estos requisitos a todo desarrollo, mantenimiento o modificación contratado con terceros. Evidencia: contrato, anexos técnicos, cláusulas de seguridad y matriz de requisitos contractuales.
- Establecer contractualmente la remediación de vulnerabilidades identificadas en software desarrollado por terceros mediante cláusulas que obliguen a corregir los hallazgos de seguridad detectados durante las evaluaciones institucionales, sin costos adicionales para la entidad cuando correspondan al desarrollo contratado. Exigir la corrección antes de la aceptación o puesta en producción, de acuerdo con la criticidad

definida. Evidencia: cláusula contractual, reporte de vulnerabilidades, plan de remediación, evidencias de corrección y resultados de validación.

- Verificar y certificar las evidencias de seguridad entregadas por el desarrollador externo mediante listas de verificación, revisión documental, análisis técnicos y validación de resultados de pruebas, antes de aceptar los entregables y cuando se realicen modificaciones significativas al software. Evidencia: lista de verificación, informe de validación, certificación de cumplimiento y expediente técnico del desarrollo.
- Validar la ausencia de contenido malicioso intencional o no intencional mediante análisis automatizados y manuales del código fuente, componentes, librerías, paquetes y artefactos entregados, utilizando herramientas de detección de malware, análisis de comportamiento y revisión de dependencias. Realizar las validaciones antes de la entrega y puesta en producción. Evidencia: reportes de análisis, resultados de herramientas de seguridad, registros de hallazgos y certificación de resultados.
- Verificar la ausencia o tratamiento de vulnerabilidades conocidas mediante análisis SAST, DAST, análisis de dependencias, revisión de componentes y consulta de bases de vulnerabilidades aplicables a las tecnologías utilizadas. Ejecutar las pruebas antes de la aceptación y repetirlas después de cambios significativos o ante la identificación de nuevas vulnerabilidades críticas. Evidencia: informes de vulnerabilidades, resultados SAST/DAST, inventario de componentes, registros de remediación y resultados de revalidación.
- Ejecutar y validar pruebas de seguridad estáticas y dinámicas mediante herramientas SAST y DAST integradas al ciclo de desarrollo, complementadas con pruebas manuales cuando la criticidad o naturaleza

del sistema lo requiera. Realizar las pruebas antes de la aceptación y puesta en producción, y repetirlas ante cambios relevantes. Evidencia: reportes SAST/DAST, casos de prueba, resultados obtenidos, vulnerabilidades identificadas y evidencias de corrección.

- Verificar la entrega completa de documentación, componentes y artefactos del desarrollo mediante una lista de entrega que incluya código fuente, ejecutables, librerías, configuraciones, documentación técnica y funcional, modelos de datos, scripts, manuales y demás elementos requeridos para su operación y mantenimiento. Realizar la validación antes de formalizar la aceptación del desarrollo. Evidencia: acta o lista de entrega, repositorios, paquetes de instalación, documentación técnica y registro de aceptación.
- Exigir y verificar la aplicación de prácticas de desarrollo seguro mediante la incorporación en los requisitos técnicos y contractuales de metodologías y controles basados, como mínimo, en OWASP y en principios de Secure Software Development Lifecycle (SSDLC), incluyendo gestión de vulnerabilidades, revisión de código, análisis de dependencias, pruebas de seguridad y remediación. Verificar su aplicación durante las etapas del desarrollo y antes de la aceptación del producto. Evidencia: metodología aplicada, matriz de cumplimiento OWASP/SSDLC, resultados de revisiones, reportes de pruebas y certificación de cumplimiento.

8.15.8. Separación de entornos de desarrollo, prueba y producción

Control Asociado en el MSPI: 8.31

Proteger el entorno de producción y datos de riesgos derivados de actividades de desarrollo y prueba. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Implementar controles para prevenir accesos y modificaciones no autorizadas en los ambientes del ciclo de vida del desarrollo mediante segregación de funciones, perfiles diferenciados, autenticación, mínimo privilegio, control de cambios y registro de actividades. Aplicar estos controles de manera permanente y revisarlos ante cambios en la arquitectura o en el ciclo de desarrollo. Evidencia: matriz de accesos, configuraciones de seguridad, registros de autenticación, logs y revisiones de permisos.
- Mantener segregados los ambientes de desarrollo, pruebas y producción mediante redes, servidores, repositorios, credenciales y perfiles de acceso diferenciados, estableciendo controles específicos para el intercambio de información entre ambientes. Mantener la segregación durante todo el ciclo de vida y verificarla antes de cada puesta en producción. Evidencia: diagramas de arquitectura, reglas de firewall, configuraciones, matriz de accesos y resultados de verificaciones.
- Restringir las herramientas de desarrollo en producción mediante la eliminación o deshabilitación de compiladores, editores de código, intérpretes, herramientas de depuración, código fuente y utilitarios que no sean necesarios para la operación. Verificar su ausencia durante la implementación y mediante revisiones periódicas de configuración. Evidencia: inventarios de software, configuraciones de servidores, resultados de escaneos y listas de verificación.
- Controlar el intercambio de información entre ambientes mediante repositorios autorizados, mecanismos de transferencia seguros, validación de archivos, control de acceso, trazabilidad y autorización previa cuando corresponda. Aplicar estos controles en cada transferencia

de información entre desarrollo, pruebas y producción. Evidencia: registros de transferencia, autorizaciones, logs, hashes y trazabilidad de archivos.

- Asignar accesos diferenciados para cada ambiente mediante identidades individuales, perfiles específicos y privilegios mínimos, evitando el uso de credenciales compartidas entre desarrollo, pruebas y producción. Revisar los permisos periódicamente y ante cambios de funciones o roles. Evidencia: matriz de accesos, registros de autenticación, configuraciones de perfiles y resultados de revisiones.
- Validar que los desarrollos institucionales se ejecuten en plataformas autorizadas mediante repositorios, herramientas y ambientes de desarrollo institucionalmente habilitados, restringiendo la utilización de plataformas no autorizadas para almacenar o procesar código institucional. Realizar la validación durante el desarrollo y antes de integrar los componentes a los ambientes de prueba o producción. Evidencia: inventario de plataformas autorizadas, registros de repositorios, logs de acceso y resultados de verificaciones.
- Integrar nuevas aplicaciones misionales y plataformas de manera controlada mediante evaluación de compatibilidad, análisis de impacto, pruebas de integración, validación de dependencias y verificación de capacidad, seguridad y conectividad con la infraestructura existente. Realizar estas validaciones antes de la puesta en producción. Evidencia: análisis de impacto, resultados de pruebas, diagramas de integración, actas de aprobación y registros de despliegue.
- Controlar la transferencia de software entre ambientes mediante un procedimiento que establezca criterios de autorización, revisión de código, pruebas, control de versiones, validación de seguridad, empaquetado, integridad, trazabilidad y reversión. Aplicar el

procedimiento en cada promoción de software hacia producción. Evidencia: procedimiento vigente, solicitudes de cambio, aprobaciones, registros de versiones, hashes y evidencias de despliegue.

- Validar los cambios antes de su implementación en producción mediante pruebas en un ambiente segregado, evaluación de resultados, revisión de seguridad y aprobación formal del cambio. Aplicar este control a todo cambio, excepto los cambios de emergencia debidamente justificados, autorizados y registrados, cuya ejecución no comprometa la continuidad del negocio. Evidencia: solicitud de cambio, resultados de pruebas, aprobaciones, registros de implementación y, para emergencias, justificación y evidencia de validación posterior.
- Restringir el acceso a compiladores, editores, depuradores y utilitarios de desarrollo desde producción mediante controles de instalación, listas de software autorizado, políticas de ejecución y permisos administrativos. Revisar periódicamente los equipos y servidores productivos para detectar herramientas no autorizadas. Evidencia: inventarios de software, políticas de ejecución, reportes de escaneo y registros de excepciones.
- Aplicar perfiles diferenciados entre ambientes de pruebas y producción mediante identidades, roles, permisos y mecanismos de autenticación independientes, evitando que las credenciales utilizadas en pruebas otorguen acceso directo a producción. Verificar la segregación durante la creación de cuentas, cambios de roles y revisiones periódicas de acceso. Evidencia: matriz de perfiles, configuraciones de acceso, registros de autenticación y resultados de revisión.
- Controlar la presentación de información en las interfaces de los sistemas mediante mensajes, menús, etiquetas e identificadores que permitan distinguir claramente el ambiente de desarrollo, pruebas y

producción y reduzcan el riesgo de ejecutar operaciones en el ambiente equivocado. Verificar esta diferenciación durante las pruebas y antes de cada puesta en producción. Evidencia: capturas de pantalla, casos de prueba, listas de verificación y resultados de validación.

- Restringir el uso de datos personales en ambientes de desarrollo y pruebas mediante anonimización, seudonimización, enmascaramiento o generación de datos sintéticos, evitando utilizar información real salvo que exista una justificación y controles de protección aplicables conforme a la Ley 1581 de 2012. Aplicar estas medidas antes de transferir datos desde producción hacia ambientes no productivos. Evidencia: autorización de uso, procedimientos de anonimización/enmascaramiento, registros de transferencia y resultados de verificación.
- Implementar controles de acceso a los ambientes de desarrollo seguro mediante autenticación individual, mínimo privilegio, segregación de funciones, controles de red y gestión formal de altas, modificaciones y bajas de usuarios. Revisar periódicamente los accesos y revocarlos cuando dejen de ser necesarios. Evidencia: matriz de accesos, registros de autenticación, configuraciones de red, solicitudes de acceso y reportes de revisión.
- Monitorear y registrar los cambios realizados en los ambientes de desarrollo y repositorios de código fuente mediante sistemas de control de versiones, registros de auditoría, control de ramas y mecanismos de gestión de cambios. Realizar seguimiento continuo y revisar los registros ante cambios críticos o eventos de seguridad. Evidencia: logs, solicitudes de cambio, bitácoras y reportes de auditoría.
- Proteger las copias de respaldo de los ambientes de desarrollo mediante repositorios independientes, cifrado, control de acceso, retención

definida y separación física o lógica respecto del entorno de desarrollo. Ejecutar las copias conforme al esquema de respaldo definido y verificar periódicamente su integridad y capacidad de restauración. Evidencia: registros de backup, configuración de almacenamiento, reportes de éxito, pruebas de restauración y registros de integridad.

- Monitorear y controlar la información transferida desde y hacia los ambientes de desarrollo mediante controles de acceso, registros de transferencia, DLP cuando aplique, validación de archivos, canales seguros y mecanismos de detección de información sensible. Aplicar los controles en cada transferencia y generar alertas ante operaciones no autorizadas. Evidencia: logs de transferencia, alertas DLP, registros de autorización, reportes de monitoreo y evidencias de atención.
- Aplicar nuevamente el control de validación previa de cambios a producción mediante pruebas en ambientes segregados, revisión de resultados y aprobación formal antes del despliegue. Exceptuar únicamente cambios de emergencia debidamente justificados y registrados, realizando posteriormente la validación y documentación correspondiente. Evidencia: tickets de cambio, resultados de pruebas, aprobaciones, registros de despliegue y evidencias de revisión posterior.
- Validar el uso exclusivo de plataformas institucionales autorizadas para el desarrollo mediante controles sobre repositorios, herramientas, ambientes y accesos, restringiendo el almacenamiento o procesamiento de código institucional en plataformas no autorizadas. Realizar verificaciones durante el desarrollo y antes de la transferencia del software a pruebas o producción. Evidencia: inventario de plataformas autorizadas, registros de repositorios, logs de acceso y resultados de las verificaciones.

8.15.9. Gestión de cambios

Control Asociado en el MSPI: 8.32

Controlar los cambios que se presenten sobre los sistemas de información, aplicativos y/o servicios de la entidad a través de la definición de procedimientos formales de control de cambios a la infraestructura tecnológica de la entidad y dentro del ciclo de vida de desarrollo. Por lo tanto, se desarrollarán las siguientes actividades:

La SIDT

- Controlar las modificaciones a los paquetes de software suministrados por proveedores mediante la evaluación previa de la necesidad, impacto, compatibilidad e integridad del paquete, limitando los cambios a aquellos técnicamente justificados y sometiéndolos al proceso formal de gestión de cambios. Aplicar este control antes de cualquier modificación y registrar cada ajuste realizado. Evidencia: solicitud de cambio, análisis de impacto, autorización, registro de modificaciones y resultados de pruebas.
- Mantener actualizado el procedimiento de gestión de cambios de TI mediante revisiones periódicas, incorporación de lecciones aprendidas, resultados de auditorías, incidentes y cambios tecnológicos o normativos. Realizar la revisión al menos una vez al año y cuando se presenten cambios significativos en el proceso. Evidencia: procedimiento vigente, historial de versiones, registros de revisión y aprobaciones.
- Gestionar los cambios de TI mediante una herramienta centralizada que permita registrar solicitudes, evaluar riesgos, gestionar aprobaciones, programar actividades, controlar pruebas, documentar implementaciones, ejecutar reversas y realizar el cierre. Utilizar la herramienta para todos los cambios que afecten infraestructura,

sistemas, aplicaciones o servicios de TI. Evidencia: registros electrónicos de cambios, flujos de aprobación, bitácoras, reportes y trazabilidad.

- Medir la gestión de cambios mediante indicadores que permitan evaluar, como mínimo, cambios exitosos, cambios fallidos, cambios de emergencia, cambios reversados, incidentes derivados de cambios, cumplimiento de ventanas y tiempos de implementación. Analizar los indicadores periódicamente para identificar desviaciones y establecer acciones de mejora. Evidencia: tablero de indicadores, informes de gestión, análisis de tendencias y planes de mejora.
- Verificar la integridad de los paquetes de software suministrados por proveedores mediante hashes, firmas digitales, certificados, mecanismos de verificación de integridad o controles equivalentes antes de su instalación. Realizar la validación antes de cada instalación o actualización. Evidencia: hash o firma verificada, certificado, registro de validación y evidencia de la versión instalada.
- Incorporar criterios de seguridad al proceso de gestión de cambios mediante la evaluación de confidencialidad, integridad, disponibilidad, autenticación, accesos, vulnerabilidades, continuidad y protección de datos. Aplicar los criterios durante la evaluación de cada cambio según su nivel de riesgo. Evidencia: análisis de impacto y riesgo, lista de verificación de seguridad y aprobación del cambio.
- Gestionar formalmente cada cambio de TI mediante las etapas de registro, planificación, evaluación, autorización, pruebas, implementación, validación y cierre. Aplicar el flujo completo a todo cambio normal y utilizar un flujo controlado para cambios de emergencia debidamente justificados. Evidencia: ticket o FRC, aprobaciones, resultados de pruebas, registros de implementación, validación y cierre.
- Registrar las solicitudes de cambio mediante el Formato de

Requerimiento de Cambio (FRC) o la herramienta institucional de gestión, incluyendo descripción, justificación, alcance, impacto, riesgo, fecha propuesta, responsables técnicos, plan de pruebas y reversión. Generar el registro antes de iniciar cualquier cambio normal. Evidencia: FRC o ticket de cambio completo y trazable.

- Programar las ventanas de cambio mediante un calendario de cambios que registre fecha, hora, duración estimada, servicios afectados y actividades previstas, acompañado del plan de interrupción cuando exista indisponibilidad. Publicar y aprobar la programación antes de ejecutar el cambio. Evidencia: calendario de cambios, plan de interrupción, comunicaciones y aprobación de la ventana.
- Evaluar el impacto y riesgo de los cambios mediante criterios de misionalidad, seguridad, complejidad, experiencia técnica, capacidad, disponibilidad, continuidad, criticidad, dependencias y afectación a los procesos. Realizar la evaluación antes de autorizar el cambio y actualizarla cuando se modifique su alcance. Evidencia: matriz de riesgo e impacto, concepto técnico, clasificación del cambio y aprobación.
- Probar los cambios en ambientes controlados mediante ambientes de prueba segregados y representativos de producción, utilizando casos de prueba funcionales, técnicos y de seguridad. Completar las pruebas y obtener las aprobaciones correspondientes antes de implementar el cambio en producción. Evidencia: plan de pruebas, resultados, evidencias técnicas, aprobación técnica y aceptación funcional.
- Implementar los cambios autorizados mediante órdenes de trabajo, tickets o mecanismos equivalentes que permitan rastrear las actividades ejecutadas, respetando la fecha y ventana aprobadas y aplicando el plan de reversión previamente definido. Ejecutar únicamente cambios aprobados y documentar cualquier desviación ocurrida durante la

implementación. Evidencia: orden de trabajo, bitácora de implementación, aprobación, plan de reversión y registros técnicos.

- Ejecutar el plan de reversión mediante procedimientos previamente probados que permitan restaurar la configuración, versión o servicio anterior cuando el cambio genere fallas, incumpla los criterios de aceptación o afecte la continuidad. Activarlo conforme a los criterios definidos en la aprobación del cambio. Evidencia: plan de reversión, registros de ejecución, resultados de recuperación y validación del servicio.
- Realizar la revisión posterior a la implementación mediante la comparación de los resultados obtenidos frente a los objetivos y criterios de aceptación, verificando impactos no previstos, satisfacción de las partes interesadas y necesidad de acciones adicionales. Ejecutar la revisión después de los cambios de acuerdo con su criticidad y cerrar formalmente el registro. Evidencia: evaluación postimplementación, acta o registro de cierre, validación de resultados y acciones correctivas.
- Documentar las lecciones aprendidas mediante el análisis de incidentes, desviaciones, dificultades, resultados y oportunidades de mejora identificadas durante la implementación. Realizar este análisis cuando el cambio sea significativo, falle, sea reversado o genere impactos no previstos. Evidencia: informe de lecciones aprendidas, acciones de mejora y actualización de procedimientos.
- Validar la afectación de los procesos de negocio mediante pruebas funcionales posteriores al cambio y confirmación de los criterios de aceptación establecidos. Realizar la validación inmediatamente después de la implementación y antes del cierre del cambio. Evidencia: resultados de pruebas, aceptación funcional, acta de conformidad y registro de cierre.

- Mantener actualizado el inventario de sistemas y software mediante un registro centralizado que incluya nombre, versión, fecha de compilación o liberación, estado, componentes relevantes y datos necesarios para su mantenimiento y soporte. Actualizarlo con cada nueva versión, cambio significativo o incorporación de software. Evidencia: inventario actualizado, historial de versiones y registros de actualización.
- Restringir el acceso a documentación técnica, código fuente, bibliotecas y ejecutables mediante controles de acceso basados en roles, mínimo privilegio, autenticación individual y registro de actividades. Revisar periódicamente los permisos y mantener únicamente los accesos necesarios; exceptuar la documentación destinada a usuarios finales. Evidencia: matriz de accesos, permisos de repositorios, logs y reportes de revisión.
- Verificar la integridad de las aplicaciones después de cambios en las plataformas operativas mediante pruebas funcionales, de integración, seguridad y validación de dependencias. Realizar las verificaciones antes y después de cambios relevantes en sistemas operativos, bases de datos, middleware o infraestructura. Evidencia: resultados de pruebas, listas de verificación, informes de impacto y registros de validación.
- Programar los cambios de plataforma con anticipación mediante un calendario coordinado con las ventanas de prueba, validación y despliegue, garantizando tiempo suficiente para ejecutar pruebas y aplicar reversión. Realizar la programación antes de la fecha prevista de implementación. Evidencia: calendario de cambios, cronograma, plan de pruebas y aprobaciones.

Modificación de paquetes de software

- Evaluar el riesgo de modificar paquetes de software mediante análisis

de integridad, compatibilidad, seguridad, soporte, impacto operativo y afectación de controles existentes. Realizar la evaluación antes de autorizar cualquier modificación. Evidencia: análisis de riesgo, evaluación de impacto y autorización.

- Validar la autorización del proveedor para modificar paquetes suministrados externamente mediante solicitud formal de permiso, documentación técnica y mecanismos de certificación o validación de integridad. Obtener la autorización antes de realizar modificaciones que puedan afectar las condiciones de soporte o integridad del producto. Evidencia: autorización del proveedor, certificado, comunicaciones y documentación técnica.
- Documentar y aprobar toda modificación de software mediante una solicitud de cambio que registre la justificación, alcance, componentes afectados, riesgos, pruebas, aprobación y plan de reversión. Obtener la aprobación correspondiente antes de implementar el ajuste. Evidencia: solicitud de cambio, aprobación, comité o registro de decisión y documentación técnica.
- Evaluar el impacto de las modificaciones sobre el mantenimiento futuro mediante análisis de soporte, actualización, compatibilidad, dependencia de proveedores y esfuerzo requerido para mantener la solución modificada. Realizar la evaluación antes de aceptar modificaciones que generen responsabilidades adicionales de mantenimiento. Evidencia: análisis de impacto, concepto técnico y registro de decisión.
- Validar la compatibilidad con otros sistemas y componentes mediante pruebas de integración, revisión de dependencias, interfaces, versiones y protocolos utilizados. Realizar las pruebas antes de implementar el paquete modificado en producción. Evidencia: matriz de compatibilidad, resultados de pruebas y reportes de integración.

- Documentar y probar integralmente las modificaciones mediante procedimientos reproducibles, control de versiones, casos de prueba y documentación técnica que permita replicar el cambio en futuras actualizaciones. Conservar esta información durante todo el ciclo de vida del software. Evidencia: código versionado, scripts, procedimientos de instalación, casos de prueba y documentación técnica.

Controles complementarios

- Validar que todo cambio de infraestructura o sistemas de información cuente con una solicitud formal mediante el FRC o herramienta institucional de gestión y ejecutar las actividades conforme al procedimiento de gestión de cambios. Aplicar este control antes de cualquier cambio normal y documentar las excepciones de emergencia. Evidencia: solicitud de cambio, aprobaciones, registros de ejecución y cierre.
- Aplicar controles formales de documentación, especificación, pruebas, calidad e implementación mediante criterios definidos para nuevos desarrollos, nuevas funcionalidades y modificaciones significativas. Aplicarlos durante todo el ciclo de vida y antes de la puesta en producción. Evidencia: especificaciones, planes de prueba, resultados de calidad, aprobaciones y registros de despliegue.
- Aplicar los lineamientos establecidos para la gestión de cambios mediante el flujo institucional de solicitud, evaluación, aprobación, pruebas, implementación, validación, reversión y cierre. Verificar su cumplimiento en cada cambio mediante controles de trazabilidad. Evidencia: tickets, listas de verificación, registros de aprobación y auditoría.

- Controlar las actualizaciones automáticas en activos críticos mediante políticas de actualización centralizada, ventanas controladas, pruebas previas y autorización explícita, evitando actualizaciones automáticas que puedan afectar aplicaciones o servicios críticos. Aplicar las actualizaciones después de validar compatibilidad, impacto y posibilidad de reversión. Evidencia: políticas de actualización, inventario de activos críticos, registros de pruebas y autorizaciones.
- Validar el funcionamiento de las aplicaciones críticas después de cambios mediante pruebas funcionales, integración, seguridad, rendimiento y disponibilidad orientadas a verificar que no se generen impactos adversos sobre las operaciones o los activos críticos. Realizar las pruebas después de cada cambio relevante y antes del cierre del cambio. Evidencia: resultados de pruebas, criterios de aceptación, registros de monitoreo, incidencias y certificación de funcionamiento.

8.16. Política De Tratamiento Y Protección De Datos

Regula el tratamiento de los datos personales recolectados, almacenados y utilizados por la entidad, en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios. Define principios, derechos de los titulares, deberes del responsable y encargado del tratamiento, medidas de seguridad, protocolos de atención de consultas y reclamos, y mecanismos de anonimización. Aplica a todos los actores que accedan o gestionen datos personales en el marco de las funciones de la ANCP-CCE.

9. GESTIÓN DE RIESGOS

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente ha adoptado un enfoque integral para la gestión de riesgos, conforme a los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), el Departamento Administrativo de la Función Pública (DAFP), y estándares internacionales como la norma ISO 31000:2018. Este enfoque se materializa

en la Política del Sistema de Administración de Riesgos, la cual establece las fases, responsabilidades y criterios para identificar, valorar, tratar y monitorear los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

La gestión del riesgo se aplica de manera transversal a todos los procesos y modelos implementados en la entidad, incluyendo los relacionados con la seguridad y privacidad de la información. Se estructura en tres líneas de defensa, con responsabilidades claramente definidas para la alta dirección, los líderes de procesos, el equipo de planeación y el control interno. Las fases del proceso incluyen el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo.

Los riesgos se valoran con base en su probabilidad e impacto, y se clasifican en zonas de riesgo (bajo, moderado, alto y extremo), lo que permite priorizar su tratamiento. Las opciones de tratamiento incluyen evitar, mitigar, transferir o asumir el riesgo, salvo en el caso de riesgos de corrupción, los cuales no pueden ser asumidos en ninguna circunstancia.

Para más detalle sobre la metodología, criterios de valoración, niveles de aceptación y responsabilidades específicas, se debe consultar el manual del Sistema de Administración de Riesgos CCE-DES-MA-02, documento que constituye la metodología oficial para la gestión de riesgos en la entidad.

10. INDUCCIÓN, CAPACITACIÓN Y DESARROLLO DE COMPETENCIAS

Con el fin de fortalecer las competencias del talento humano en materia de seguridad y privacidad de la información, la ANCP-CCE establece un enfoque estructurado de formación continua, alineado con la Guía 14 del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Plan Institucional de Capacitación (PIC).

10.1. Inducción

Todo nuevo funcionario o contratista debe recibir una inducción obligatoria que incluya:

- Introducción al MSPI.
- Políticas de seguridad y privacidad de la información.
- Uso adecuado de recursos tecnológicos.
- Responsabilidades individuales frente a la protección de la información.
-

10.2. Capacitación Continua

La capacitación se organiza en ciclos trimestrales, abordando los temas definidos por el MSPI:

- Primer trimestre: administración de contraseñas, política de escritorio limpio, roles y responsabilidades, uso apropiado de internet.
- Segundo trimestre: malware y tipos, software permitido/prohibido, spam y correos sospechosos, shoulder surfing.
- Tercer trimestre: gestión de incidentes, backups y recuperación, cambios en sistemas, amenazas y vulnerabilidades comunes.
- Cuarto trimestre: ingeniería social, control de acceso, uso de dispositivos fuera de la entidad, políticas organizacionales.
- Estas capacitaciones se desarrollan mediante sesiones virtuales, talleres prácticos, cursos e-learning, boletines informativos y simulacros.

10.3. Sensibilización y Comunicación

Se implementan campañas periódicas para reforzar buenas prácticas, mediante:

- Boletines mensuales.

- Infogramas temáticos.
- Charlas con expertos.
- Simulacros de phishing.
-

10.4. Entrenamiento Especializado

Dirigido al Grupo de Seguridad y Privacidad de la Información, incluye:

- Fundamentos de ciberseguridad.
- Gestión de riesgos digitales.
- Protección de datos personales.
- Normativas y estándares aplicables.

10.5. Evaluación y Mejora Continua

Se aplican mecanismos de evaluación como cuestionarios, encuestas y análisis de indicadores de participación y desempeño. Los resultados permiten retroalimentar y ajustar el plan de formación anualmente.

10.6. Integración con el PIC

Este componente se articula con el Plan Institucional de Capacitación (PIC), garantizando:

- Inclusión de los temas MSPI como línea transversal.
- Priorización de grupos según nivel de exposición a riesgos.
- Asignación de recursos y tiempos en el cronograma anual.

11. PREPARACION Y RESPUESTA ANTE EMERGENCIAS

Control Asociado en el MSPI: 5.24 a 5.30 y 8.13 a 8.16

Establecer los lineamientos para preparar, prevenir, responder y recuperarse ante situaciones de emergencia que puedan afectar la confidencialidad, integridad o disponibilidad de la información, los servicios tecnológicos, las

instalaciones, los sistemas de información y demás activos de información de la Entidad.

La preparación y respuesta ante emergencias debe permitir una actuación coordinada, oportuna y documentada, reduciendo los impactos sobre la operación institucional y garantizando, en la medida de lo posible, la continuidad de los procesos y servicios críticos.

11.1. Alcance

Aplica a todos los procesos, servidores públicos, contratistas, terceros, sistemas de información, infraestructura tecnológica, instalaciones y activos de información que hagan parte del SGSI.

Comprende emergencias originadas por eventos naturales, tecnológicos, humanos, físicos o de ciberseguridad, incluyendo, entre otros:

- Incendios, inundaciones, terremotos u otras amenazas naturales.
- Fallas prolongadas de energía eléctrica, climatización o comunicaciones.
- Daños en centros de datos o infraestructura tecnológica.
- Indisponibilidad de sistemas o servicios críticos.
- Incidentes de ciberseguridad que afecten la operación.
- Ataques de ransomware, malware o denegación de servicio.
- Compromiso de cuentas privilegiadas o sistemas críticos.
- Pérdida, daño o destrucción de equipos o medios de almacenamiento.
- Alteraciones graves de las instalaciones físicas.
- Situaciones que requieran evacuación o traslado de personal.
- Fallas o indisponibilidad de proveedores tecnológicos críticos.

11.2. Identificación y evaluación de escenarios de emergencia

La ANCP-CCE debe identificar periódicamente los escenarios que puedan generar interrupciones o afectaciones significativas a la seguridad de la información y a la continuidad de los procesos.
Los escenarios deben estar articulados con la gestión de riesgos de seguridad de la información, el análisis de impacto al negocio (BIA), el Plan de Continuidad del Negocio (BCP) y el Manual de Recuperación ante Desastres.

11.3. Preparación para la respuesta

La ANCP-CCE debe mantener las condiciones necesarias para responder de manera organizada ante una emergencia. Para ello debe:

- Definir responsables y roles para la atención de emergencias que puedan afectar la seguridad de la información.
- Mantener actualizados los datos de contacto de los responsables y equipos de atención.
- Establecer procedimientos de escalamiento y comunicación.
- Mantener identificados los sistemas, servicios y activos críticos.
- Las responsabilidades deben ser las siguientes:

Tabla 2: Roles y responsabilidades ante emergencias

Rol	Responsabilidades
Alta Dirección	Aprobar recursos, declarar emergencias críticas y supervisar la recuperación.
Responsable del SGSI	Coordinar la respuesta, activar procedimientos, realizar seguimiento y reportar el incidente.
Área de Tecnología	Recuperar la infraestructura tecnológica y restaurar los servicios afectados.

Equipo de Seguridad de la Información	Contener el incidente, preservar evidencias, realizar análisis técnico y coordinar la gestión del incidente de seguridad.
Responsables de Proceso	Informar afectaciones, apoyar la recuperación y validar el restablecimiento de los procesos.
Usuarios	Reportar oportunamente situaciones anómalas y cumplir las instrucciones emitidas durante la emergencia.
Proveedores Críticos	Brindar soporte conforme a los acuerdos de niveles de servicio (SLA) y a los procedimientos establecidos.

Fuente: elaboración propia

11.4. Clasificación de la emergencia

La clasificación debe considerar el impacto sobre la confidencialidad, integridad y disponibilidad, así como el impacto operativo, legal, financiero y reputacional.

Los niveles establecidos serán los siguientes:

Tabla 3: Clasificación de emergencias

Nivel	Denominación	Descripción	Acciones Principales
Nivel 1	**Emergencia Baja**	Evento con impacto limitado que afecta activos o servicios no críticos y puede ser atendido por el área responsable sin comprometer la operación institucional.	Atención por el área responsable, registro del evento y seguimiento hasta su cierre.
Nivel 2	**Emergencia Media**	Evento que afecta uno o varios servicios importantes o genera un riesgo moderado para la información, requiriendo la coordinación de varias áreas para su atención.	Escalamiento al responsable del SGSI, coordinación técnica entre las áreas involucradas y aplicación de medidas de contención y recuperación.

Nivel 3	**Emergencia Alta**	Evento que compromete procesos o activos críticos de información, afectando significativamente la continuidad de las operaciones y requiriendo la activación de planes de contingencia.	Activación del Plan de Continuidad del Negocio y/o del Plan de Recuperación ante Desastres, participación del Comité de Gestión de Incidentes y comunicación a la Alta Dirección.
Nivel 4	**Emergencia Crítica**	Evento de máximo impacto que pone en riesgo la operación institucional, compromete múltiples servicios críticos o genera afectaciones graves a la información, la infraestructura o la reputación de la Entidad.	Activación del Comité de Crisis, ejecución integral de los planes de continuidad y recuperación, coordinación con proveedores y, cuando corresponda, notificación a las autoridades competentes.

Fuente: elaboración propia

11.5. Activación de la respuesta

Ante la identificación de una emergencia, el responsable que detecte o reciba la alerta debe:

- Reportar inmediatamente el evento por los canales establecidos.
- Registrar la información disponible sobre el evento.
- Determinar preliminarmente el alcance y nivel de afectación.
- Informar al responsable de seguridad de la información y/o al equipo correspondiente.
- Activar el procedimiento de gestión de incidentes cuando corresponda.
- Escalar la situación cuando pueda afectar procesos o servicios críticos.
- Activar los procedimientos de continuidad o recuperación cuando se superen los niveles establecidos.
- Mantener evidencia de las decisiones y acciones ejecutadas.

La activación de mecanismos de emergencia debe realizarse bajo criterios previamente definidos y siguiendo las recomendaciones establecidas en los documentos:

- CCE-SGI-PL-05 Manual de recuperación ante desastres
- CCE-SGI-PL-04 Plan de continuidad del negocio (BCP) para las plataformas de la ANCP-CCE

11.6. Respuesta ante emergencias

Durante la atención de una emergencia se deben priorizar las siguientes acciones:

Protección de las personas

La protección de la vida y la integridad de las personas tendrá prioridad sobre la protección de los activos tecnológicos o de información.

Cuando exista riesgo para las personas, deben aplicarse los procedimientos institucionales de emergencia y evacuación correspondientes.

Contención

Una vez controlado el riesgo para las personas, se deben implementar medidas para evitar que el evento continúe afectando la información o los servicios.

Estas medidas pueden incluir:

- Aislamiento de equipos o redes.
- Suspensión temporal de servicios.
- Bloqueo de cuentas comprometidas.
- Desconexión de sistemas afectados.
- Activación de mecanismos alternos.
- Restricción de accesos físicos o lógicos.
- Protección de copias de seguridad.
- Preservación de evidencias.

Continuidad

Cuando la emergencia genere indisponibilidad de servicios críticos, deben activarse los mecanismos definidos en el Plan de Continuidad del Negocio y/o Plan de Recuperación ante Desastres, de acuerdo con los criterios establecidos.

La recuperación debe priorizar los servicios de acuerdo con su criticidad, RTO, RPO y dependencias.

11.7. Gestión de la información durante la emergencia

Durante una situación de emergencia se debe garantizar, en la medida de lo posible, la protección de la información.

Se deben considerar como mínimo los siguientes aspectos:

- Mantener la confidencialidad de la información durante la contingencia.
- Evitar la divulgación no autorizada de información relacionada con la emergencia.
- Controlar los accesos físicos y lógicos a los recursos afectados.
- Mantener mecanismos de autenticación y autorización cuando sea posible

11.8. Comunicación durante la emergencia

La comunicación debe realizarse de manera oportuna, controlada y por canales previamente establecidos.

Se deben definir:

- Responsables de comunicación.
- Canales primarios y alternos.
- Contactos internos y externos.
- Mecanismos de escalamiento.

11.9. Recuperación y retorno a la operación normal

Una vez controlada la emergencia, se debe realizar la recuperación progresiva de los servicios afectados.

Como mínimo se debe:

Confirmar que las condiciones para la recuperación sean seguras. integridad de la infraestructura y los servicios de acuerdo con su prioridad. información utilizando copias de seguridad confiables.

12. CONTROL DE PROVEEDORES Y CONTRATISTAS

La organización debe establecer y comunicar una política específica del tema sobre las relaciones con los proveedores a todas las partes interesadas relevantes. La organización debería identificar e implementar procesos y procedimientos para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Esto también debería aplicarse al uso que hace la organización de los recursos de los proveedores de servicios en la nube. Estos procesos y procedimientos deben incluir los que debe implementar la organización, así como aquellos que la organización requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor.

Los acuerdos con los proveedores deben establecerse y documentarse para garantizar que haya un entendimiento claro entre la organización y el proveedor con respecto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.
El seguimiento, la revisión y la gestión de cambios de los servicios del proveedor deben garantizar que se cumplan los términos y condiciones de seguridad de la información de los acuerdos, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente y que los cambios en los servicios del proveedor o el estado comercial no afecten la prestación del servicio.

13. MEDICIÓN Y SEGUIMIENTO

La creación de indicadores de gestión está orientada principalmente a la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:
Evaluar la efectividad de la implementación de los controles de seguridad.
Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.

Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
Comunicar valores de seguridad al interior de la entidad.
Servir como insumos al plan de análisis y tratamiento de riesgos.
Permitir que se cuente con un proceso que demuestre si está siendo eficaz y está llegando a su punto de equilibrio dentro del sistema de gestión de seguridad de la información.

14. GESTIÓN DE CAMBIOS

La gestión del cambio en el Subsistema de Seguridad y Privacidad tiene como propósito asegurar que toda modificación que impacte la operación, los procesos institucionales o el tratamiento de la información se realice de manera planificada, controlada y articulada con el Sistema Integrado de Gestión. Su aplicación garantiza que los cambios no comprometan la seguridad, la privacidad, la continuidad del servicio ni el cumplimiento de la normatividad vigente.

Cada cambio debe ser identificado, analizado y documentado en relación con su origen, alcance y efectos sobre los procesos institucionales. Para ello, se

consideran las fuentes derivadas de auditorías internas o externas, el seguimiento a los planes de mejoramiento, las alertas generadas en el plan de acción y las actualizaciones normativas o tecnológicas que exijan ajustes en el subsistema.

El análisis de los cambios contempla la evaluación de riesgos en seguridad y privacidad, la identificación de impactos sobre los procesos, servicios y activos de información, así como la definición de controles preventivos y correctivos que garanticen su adecuada implementación. Dicho análisis se documenta y se integra al seguimiento del Sistema Integrado de Gestión, fortaleciendo la trazabilidad y la transparencia institucional.

La planeación de los cambios debe contemplar actividades, recursos, cronogramas y mecanismos de comunicación, de manera que se asegure la correcta socialización en los procesos impactados. Cuando un cambio surja como medida correctiva o de mejora, este debe ser incorporado a los planes de mejoramiento o al plan de acción institucional, según corresponda, con el fin de mantener la alineación y coherencia con las metas estratégicas de la entidad.

La implementación de los cambios debe realizarse conforme a lo planificado, garantizando que se verifique la efectividad de los controles de seguridad y privacidad definidos. En caso de que se requiera, podrán aplicarse pruebas piloto o validaciones técnicas que aseguren la confiabilidad del resultado antes de su adopción definitiva en los procesos institucionales.

El seguimiento posterior a la implementación tiene como finalidad confirmar que el cambio cumple con los objetivos definidos y que no genera incidentes o vulnerabilidades adicionales. Para ello, se registran los resultados obtenidos, se ajustan las matrices de riesgos, se actualizan las políticas o procedimientos necesarios y se incluyen las lecciones aprendidas en los instrumentos de mejora continua.

Finalmente, el cierre de cada cambio se formaliza mediante la documentación de su resultado y su integración en el Sistema Integrado de Gestión. Esto permite consolidar la trazabilidad, retroalimentar los procesos institucionales y

garantizar que las mejoras en materia de seguridad y privacidad se traduzcan en una gestión más eficiente, transparente y confiable.

Autores y responsables del documento				
ACCIÓN	NOMBRE	CARGO	FECHA	FIRMA
Elaboró:	Oscar Sanabria C.	Contratista Seguridad de la información – SIDT	16/09/2026	Original Firmado
Revisó:	William Efrén Pardo Garzón	Analista T2 – G6 / Subdirección de Información y Desarrollo Tecnológico	17/09/2026	Original Firmado
Aprobó	COASIC: acta de reunión	Comité de Apoyo de Seguridad de la Información y Ciberseguridad	16/09/2026	Original Firmado