2020

Colombia Compra Eficiente

MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA-COLOMBIA COMPRA EFICIENTE

TABLA DE CONTENIDO

INTRODUCCIÓN

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (en adelante, **ANCP-CCE**) reconoce la importancia de la adecuada gestión y protección de sus activos de información, por lo tanto, la Entidad por medio del Proceso de Gestión de Tecnologías de la Información y el Subproceso asociado de Gestión de la Seguridad de la información, busca proteger la Integridad, Confidencialidad y la Disponibilidad de la información que gestiona en el ejercicio de sus operaciones y en concordancia con el objeto misional de la Entidad.

OBJETIVO

El presente Manual de Seguridad y Privacidad de la Información tiene como objetivo establecer los lineamientos y el marco de referencia para la adecuada gestión de la Seguridad y Privacidad de la Información al interior de la ANCP-CCE con el fin de mitigar, prevenir y evitar que se comprometa la Confidencialidad, Integridad y Disponibilidad de los Activos de Información de la Entidad.

ALCANCE Y APLICABILIDAD

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:

1. 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.
2. Las Entidades de control y demás Entidades relacionadas que accedan a cualquier Activo de Información propiedad de la ANCP-CCE, independientemente de su ubicación.
3. Los procesos internos que traten Activos de información en cumplimiento de sus objetivos estratégicos.

MARCO LEGAL

Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
Ley 1266 de 2008. Disposiciones generales Habeas Data.
Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.
Ley 1712 de 2014.Transparencia y Acceso a la información Pública Nacional.
Decreto 4170 de 2011. Creación de la ANCP-CCE.
Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1083 de 2015. Único Reglamentario del Sector Función Pública, con las modificaciones y adiciones introducidas a partir de su fecha de su expedición.
Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo con las modificaciones y adiciones introducidas a partir de su fecha de su expedición

Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Copes 3701 de 2011. Lineamientos de política para Ciberseguridad y Ciberdefensa.
Copes 3854 de 2016. Política Nacional de Seguridad Digital.
Guía-Modelo de Seguridad y Privacidad de la Información MSPI- MinTIC.
Guía -Modelo de Gestión de Riesgos de Seguridad Digital -MinTIC.
NTC-ISO/IE 27001
NTC-ISO/IE 27002
BS 25999

DEFINICIONES

Activo de Información: Es la información que reside en medio electrónico o físico, que tiene un significado y valor para Colombia Compra Eficiente 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.
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.
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 deberá ser divulgada.
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
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.
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.
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 sensible: Es aquel Dato Personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación.
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
Disponibilidad: Es el principio de la Seguridad de la Información que busca asegurar que la información sea accesible y utilizable cuando sea requerida.
Incidente de Seguridad: Es un evento inesperado y no deseado que compromete la Seguridad de la Información.
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.

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.
MSPI: Modelo de seguridad y privacidad establecido por el MinTIC en el marco de la estrategia de Gobierno Digital.
Oficial de Seguridad de la Información: Es el contratista y/o funcionario que cumple la función de supervisión del cumplimiento del MISP y la Seguridad Digital dentro de la Entidad.
Privacidad: Es el ámbito de la vida privada de una persona, el cual deberá mantenerse confidencial.
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.
Política de Seguridad y Privacidad de la Información: Es el documento que establece los lineamientos y las medidas organizaciones, técnicas y físicas dentro de la Entidad para evitar, prevenir y mitigar los riesgos que comprometan la seguridad, confidencialidad, integridad y disponibilidad de los Activos de información de la ANCP-CCE.
Recurso Tecnológico: Es cualquier medio tecnológico de Colombia Compra Eficiente.
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.
Vulnerabilidad: es una debilidad en un sistema o componente tecnológico, que puede ser explotada por una amenaza para materializar un riesgo.

MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La ACNP-CCE, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y de acuerdo con lo establecido en el Subproceso de Seguridad de la Información que hace parte del proceso de Gestión de Tecnologías de la Información de la Entidad, protege, preserva y administra la Confidencialidad, Integridad y Disponibilidad de la información. A continuación, el presente documento define la(s) Política(s) y los lineamientos que conforman el presente Manual.

1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La ANCP-CCE, por medio de su Política de Seguridad y Privacidad de la Información establece el compromiso de la Entidad para evitar, prevenir y mitigar los riesgos que comprometan la Seguridad, Confidencialidad, Integridad y Disponibilidad de los Activos de información de la Entidad, así como, es el documento que establece de manera integral los lineamientos y directrices para la gestión de la seguridad de la información, los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y la Continuidad de la operación de la ANCP-CCE.

2. PROCESO GESTIÓN TECNOLOGÍAS DE LA INFORMACIÓN.

La ANCP-CCE ha definido el proceso de apoyo de Gestión de Tecnologías de Información que tiene como objetivo generar directrices y lineamientos relacionadas con la gestión de TI dentro de la Entidad, este proceso cuenta con cuatro (4) subprocesos asociados que son: Gestión de Infraestructura, Gestión de Aplicaciones, Gestión de Proyectos IT y Gestión de Seguridad de la Información, que tienen como fin atender las necesidades de la Entidad y fortalecer la gestión del cumplimiento de las metas institucionales.

3. INVENTARIO DE ACTIVOS DE INFORMACIÓN.

El grupo de seguridad y privacidad de la información, en el desarrollo de su gestión identificará y clasificará en un inventario los activos de información que son manejados por la Entidad, acorde con el alcance definido para la implementación del MSPI, respetando los principios de Confidencialidad, Integridad y Disponibilidad de cada activo y definiendo la Matriz de Activos de Información. Esta actividad deberá ser revisada de manera periódica, con el fin de determinar si un activo de información continua o no siendo parte del inventario y/o si algún valor asignado deberá modificarse. **Anexo**.

4. EVALUACIÓN Y MEDICIÓN DE EFICACIA.

Mediante la identificación, seguimiento y análisis de indicadores de Gestión, el grupo de Seguridad y Privacidad de la Información de la ANCP-CCE, medirá la efectividad, eficacia y eficiencia de la Seguridad y Privacidad de la Información en la Entidad.

5. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS.

La ANCP-CCE, mediante la implementación de la metodología de gestión de riesgos del DAFP, identificará, evaluará y gestionará los riesgos de Seguridad de la Información a los que estén expuestos los activos de información. Serán definidas la(s) Matriz de Riesgos correspondientes.[1] **Anexo**.

6. ROLES Y RESPONSABILIDADES: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La ANCP-CCE, definirá e identificará los Roles y Responsabilidades frente a la seguridad y privacidad de la información y definirá el equipo responsable de la seguridad y la privacidad de la información dentro de la Entidad. **Anexo.**

7. PLAN DE COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN.

Con el fin de generar la cultura organizacional acerca de la Seguridad y Privacidad de la Información, el Grupo de Seguridad y Privacidad de la información de la ANCP-CCE definirá el Plan de Comunicación, Sensibilización y Capacitación como complemento e insumo al Plan Institucional de Capacitación de la Entidad. **Anexo**

8. LINEAMIENTOS GENERALES PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA ANCP-CCE:

A continuación, se especificarán los lineamientos generales que la ANCP-CCE establece para la gestión de la seguridad y privacidad de la información en los diferentes escenarios en los que se trate información:

8.1 Recursos Humanos.

Objetivo: Promover que los funcionarios y/o contratistas de la ANCP-CCE cumplan con sus responsabilidades y obligaciones frente a la seguridad y privacidad de los activos de información a los que tengan acceso debido a sus funciones y/o cargos.

a) Selección de Personal.

La Secretaría General de la Entidad deberá definir un mecanismo de verificación de antecedentes para todos los candidatos (contratistas y/o funcionarios) para antes de realizar su vinculación con la Entidad y en concordancia con las Leyes aplicables.

La Secretaría General y el área de Gestión Contractual de la Entidad, deberá definir e incluir en las estipulaciones contractuales con contratistas y/o funcionarios las responsabilidades individuales y/o conjuntas en cuanto al manejo, la seguridad y privacidad que deberán tener frente a la información a la que tengan acceso debido a sus funciones o cargos.

b) Durante la ejecución del contrato.

Todos los contratistas y funcionarios de la ANCP-CCE deberán aceptar y conocer la(s) Política(s) de Seguridad y Privacidad de la Información, Tratamiento de Datos Personales y demás documentos que sean definidos por el grupo de seguridad y privacidad de la información.

El grupo de seguridad de la información de acuerdo con su Plan de Sensibilización, Capacitación y Comunicación y teniendo en cuenta el Plan Institucional de Capacitación de la Entidad, deberá fomentar la cultura y apropiación de la Seguridad y Privacidad de la Información en los contratistas y funcionarios de la Entidad.

La Secretaría General deberán implementar dentro de los procesos internos disciplinarios de la Entidad, responsabilidades y consecuencias para los contratistas y funcionarios que incurran en faltas y/o violen la seguridad y privacidad de la información, en concordancia con las Leyes aplicables.

c) Terminación del empleo y/o cambio de responsabilidad.

La Secretaria General y el área de Talento Humano de la Entidad, deberán informar a la Subdirección IDT en el menor tiempo posible, la relación correspondiente a la desvinculación, traslado de dependencia y/o cambio de funciones que se surtan periódicamente por parte de los funcionarios y contratistas de la Entidad, con el fin de retirar y configurar los permisos y accesos lógicos a los sistemas de información, activos de información, grupos de gestión, herramientas y/o aplicaciones de la Entidad.

Se deberá asegurar por parte del jefe y/o supervisor del contrato que, al momento de terminación del contrato el contratista y/o funcionario realice la entrega de los repositorios de información, claves y/o credenciales de acceso que sean propiedad de la Entidad.

Se deberá asegurar por parte del jefe y/o supervisor del contrato que, en caso de terminación anticipada, temporal y/o cesión del contrato, sea entregado la custodia del repositorio de información del contratista y/o funcionario.

El área de Secretaría General de la Entidad deberá asegurar que el contratista y/o funcionario al momento de su retiro y/o terminación de contrato realice la devolución del carné, tarjeta de lectura y/o cualquier distintivo de autenticación que lo acredite como contratista y/o funcionario de la ANCP-CCE.

8.2 Gestión de activos.

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas, con el fin de asegurar que la información de la Entidad reciba un nivel apropiado de protección evitando su divulgación, modificación, retiro y/o destrucción no autorizada.

a) Responsabilidad de los activos físicos y tecnológicos.

Al momento de su vinculación, los contratistas y funcionarios deberán ser informados acerca de los recursos tecnológicos que tienen a su disposición, así como, de los deberes, responsabilidades y compromisos que tienen sobre el uso adecuado, eficiente y ético de los mismos.

El jefe inmediato y/o el supervisor del contrato deberán velar porque los contratistas y funcionarios una vez terminada la relación laboral y/o contractual con la ANCP-CCE, devuelvan los activos de información que se encuentren a su cargo y sean propiedad de la Entidad.

La Subdirección IDT deberá identificar y documentar los lineamientos para el uso adecuado y aceptable de los activos físicos y tecnológicos asociados con la información y/o el procesamiento de información, con el fin de evitar fuga y/o divulgación de información confidencial.

La información y los activos de información a los que los funcionarios y/o contratistas de la Entidad tengan acceso debido a sus cargos o funciones son de propiedad de la ANCP-CCE y el uso de estos deberá emplearse exclusivamente con propósitos laborales y/o contractuales.

b) Identificación y clasificación de activos de información.

Bajo el liderazgo del Oficial de Seguridad de la Información de la Entidad, cada uno de los propietarios de los activos de información deberá: (i) identificar y (ii) clasificar la información de acuerdo con la metodología establecida por la ANCP-CCE y los requisitos legales vigentes y aplicables.

El oficial de Seguridad de la Información deberá liderar y coordinar el análisis de riesgos de Seguridad y Privacidad de la Información con el fin de definir las condiciones de uso y protección de los Activos de Información de la Entidad. Los propietarios de los Activos de Información deberán participar activa y responsablemente de la mano con el Oficial de Seguridad de la Información en los análisis y definición de los riesgos de Seguridad de la Información.

Los propietarios de los Activos de Información deberán revisar e implementar periódicamente los controles de seguridad que sean definidos y/o implementados para los Activos de Información de los que sean Responsables.

c) Etiquetado/Clasificación de la información.

La ANCP-CCE deberá desarrollar e implementar el esquema para el etiquetado y/o Clasificación de la información de acuerdo con la metodología de clasificación de activos adoptada por la Entidad.

Es responsabilidad de los contratistas y funcionarios de la Entidad, realizar las actividades de etiquetado y clasificación de los Activos de Información siguiendo el esquema establecido por la Entidad.

Los contratistas y funcionarios de la ANCP-CCE deberán proteger la información de la Entidad, por lo tanto, solo podrán imprimir, escanear y/o copiar documentos de la Entidad clasificados como confidenciales cuando sea estrictamente necesario.

En caso de encontrar información de la Entidad por cualquier funcionario y/o contratista sin las medidas adecuadas, se deberán resguardar, entregar a su dueño y evitar su divulgación y/o publicación no autorizada.

Los funcionarios y contratistas que generen y/o manipulen documentos físicos y/o electrónicos deberán velar que estén etiquetados de acuerdo con su nivel de Confidencialidad y los lineamientos entregados por el área de Gestión documental.

Los funcionarios y contratistas deberán conocer las estipulaciones que hace la Ley 1712 de 2014 o la ley que la modifique o reemplace, frente a la clasificación y reserva de la información.

Los funcionarios y contratistas deberán velar por la especial custodia de los documentos e información Confidencial, Clasificada y/o Reservada, ya que su inadecuado uso puede traer consigo efectos negativos a la Entidad.

d) Uso de recursos tecnológicos.

La Secretaria General y la Subdirección IDT de la Entidad deberá autorizar los movimientos y las asignaciones de los recursos tecnológicos propiedad de la ANCP-CCE, así como, promover el uso correcto de los mismos.

La Subdirección de IDT es el área encargada de instalar, reparar, actualizar y/o retirar los componentes técnicos (software/hardware) de los recursos tecnológicos de la Entidad.

La Subdirección de IDT y el grupo de infraestructura deberán implementar los procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la Entidad, así como, deberán implementar un esquema para disponer y custodiar de forma segura de los medios tecnológicos cuando ya no sean requeridos o no estén en uso.

La Subdirección de IDT y el grupo de infraestructura serán los encargados de borrar de forma segura en los casos que sea necesario, las licencias, los programas y el hardware de almacenamiento cuando sea reasignado, transferido o dispuesto a cualquier título.

Los funcionarios y contratistas deberán aceptar las condiciones e instrucciones definidas por la Subdirección de IDT y Secretaria General sobre el manejo de los recursos tecnológicos de la Entidad, así como, deberán respetar la asignación de recursos tecnológicos asignados.

Es responsabilidad de cada uno de los contratistas y funcionarios de la Entidad informar en el menor tiempo posible a la Mesa de ayuda por medio de la herramienta de gestión designada (GLPI), las fallas de las plataformas, problemas de hardware y/o software, así como las fallas, problemas e incidentes relacionados con los recursos tecnológicos de la Entidad.

El contratista y/o funcionario deberá abstenerse de solucionar, cambiar de configuración, instalar o desinstalar, formatear o restaurar de fabrica los equipos o recursos tecnológicos a su cargo que sean propiedad de la Entidad, únicamente podrá aceptar las actualizaciones del sistema que sean requeridas.

En caso de pérdida y/o robo de un recurso tecnológico propiedad de la Entidad, será responsabilidad de cada uno de los funcionarios y/o contratistas informar en el menor tiempo posible y de forma inmediata al líder de su área o dependencia, así como, al grupo de infraestructura de la Subdirección de IDT y a la Secretaria General con el fin de iniciar el trámite interno y en caso de ser necesario sean ejecutados los pasos para interponer las denuncias correspondientes ante las autoridades correspondientes.

e) Dispositivos personales

La Subdirección de IDT, el grupo de seguridad de la información y el grupo de infraestructura deberán establecer los lineamientos y escenarios en los que los funcionarios y contratistas podrán utilizar para el desarrollo de sus funciones sus dispositivos electrónicos personales para acceder a la información, red e infraestructura tecnológica de la ANCP-CCE, los lineamientos deberán establecer las reglas y obligaciones para el uso de dispositivos personales.

Los funcionarios y contratistas de la Entidad deberán evitar el envío de fotografías, audios, videos, archivos y/o información confidencial, clasificada o reservada por redes de mensajería instantánea y/o aplicaciones web que no sean las herramientas oficiales de la Entidad.

Los funcionarios y contratistas deberán evitar usar sus dispositivos móviles para acceder a la información de la ANCP-CCE en lugares que no ofrezcan garantías de seguridad física y de red, con el fin de evitar pérdida o robo y confidencialidad de la información.

Los funcionarios y contratistas de la ANCP-CCE deberán evitar conectar los dispositivos móviles institucionales asignados por el puerto USB, así como, deberán evitar conectarse a redes wifi de acceso público (hoteles, cafés internet, entre otros) para la ejecución de sus actividades contractuales.

Los funcionarios y contratistas deberán asegurar que sus dispositivos personales cuentan con las medidas de seguridad y controles necesarios cuando manejan información propiedad de la ANCP-CCE con el fin de prevenir la fuga de Información Confidencial y o Privada.

8.3 Control de acceso.

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de información. Asegurar el acceso únicamente a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios de la Entidad.

a) Identificación y autenticación individual:

La Subdirección de IDT deberá garantizar que los equipos de cómputo propiedad de la ANCP-CCE se puedan conectar y utilizar en las redes e infraestructura de la Entidad.

La Subdirección de IDT y el grupo de infraestructura deberán suministrar a los usuarios las credenciales y permisos para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, los funcionarios y contratistas son responsables de la salvaguarda de sus credenciales de usuario y las acciones realizadas con estas en las diferentes plataformas tecnológicas, servicios de red y sistemas de información de la ANCP-CCE.

Es responsabilidad de cada uno de los funcionarios y contratistas de la entidad salvaguardar la confidencialidad y privacidad de sus credenciales de acceso, así como de asegurar que su uso sea personal e intransferible.

Los funcionarios y contratistas de la Entidad deberán acogerse y cumplir con los lineamientos para la configuración de contraseñas definidos por la Subdirección de IDT, el grupo de infraestructura y el grupo de seguridad y privacidad de la información.

Los funcionarios y contratistas deberán solicitar la creación, modificación, bloqueo y/o eliminación de sus cuentas de usuario acogiéndose a los procedimientos establecidos para tal fin.

Las primeras contraseñas generadas para los funcionarios y/o contratistas para la autenticación se deberán suministrar a los usuarios por el grupo de infraestructura de la Subdirección IDT de manera segura, el sistema deberá solicitar cambio inmediato de la misma una vez se ingrese por primera vez.

La Subdirección de IDT y el grupo de infraestructura deberán establecer un procedimiento de verificación de identidad de usuarios antes de reemplazar la información secreta para la autenticación de estos y/o proporcionar una contraseña nueva temporal.

El grupo de infraestructura de la Subdirección IDT, deberá implementar y desarrollar un documento formal de control de accesos y de los sistemas de gestión de contraseñas.

b) Contraseñas y/o credenciales de acceso:

Los funcionarios y contratistas de la ANCP-CCE son responsables que sus contraseñas y/o credenciales de acceso a su cuenta o plataforma institucional (Correo, directorio activo, OneDrive, POXTA entre otros) deberá contar con tres de los siguientes elementos: (i) mayúsculas, (ii) minúsculas, (iii) números y (iv) caracteres especiales, la contraseña deberá tener una longitud mínima de 8 caracteres. El sistema deberá exigir el cambio de contraseñas en un periodo de tiempo determinado y no deberá permitir que se pueda repetir alguna de las 3 últimas contraseñas.

Al momento de definir su contraseña cada uno de los funcionarios y contratistas de la ANCP-CCE deberán seguir las siguientes recomendaciones: No utilizar información personal, palabras comunes que estén en un diccionario o enciclopedia común, el mismo nombre de usuario, secuencias de teclas predecibles o encontradas en el teclado. **Ej.**: 123456789, qwertyuiop, asdfghjklñ, abcdefghijk, etc., secuencias de letras o caracteres únicos. Ej. 1111111, aaaaaaaa, BBBBBB y/o secuencias alternadas de pocos caracteres. Ej. aSaSaS, aaAABBcc, 123aBC, etc.

c) Control y administración de acceso de usuarios a sistemas y servicios:

El grupo de infraestructura de la Subdirección IDT es el responsable de establecer el control de acceso a los datos, información y servicios para los contratistas y funcionarios de la Entidad, por lo tanto, deberá establecer un proceso formal de registro y cancelación de registro de usuarios con el fin de poder realizar la asignación de los derechos de acceso siempre aplicando el principio de menor privilegio.

El grupo de infraestructura de la Subdirección IDT deberá implementar un proceso de suministro de acceso formal de usuarios para la asignación y revocación de los derechos de acceso los sistemas y servicios y todos los usuarios de la Entidad.

El grupo de infraestructura de la Subdirección de IDT deberá establecer los controles adecuados para restringir y controlar la asignación y uso de derechos de acceso y privilegio a los recursos tecnológicos, servicios de red y los sistemas de información de la Entidad.

El grupo de infraestructura de la Subdirección de IDT deberá definir un proceso de gestión formal con el fin de definir la asignación de información de autenticación secreta.

Los propietarios de los Activos de Información son los responsables de definir los derechos de acceso, perfiles de usuarios y permisos de acceso a activos de información de la Entidad de los que sean responsables. Las solicitudes de derechos de acceso deberán realizarse por la herramienta de mesa de ayuda y el aplicativo que sea definido (GLPI), solo se otorgará el acceso solicitado a los que sean autorizados por el jefe inmediato y/o supervisor del contrato.

Los perfiles definidos en los sistemas de información y los privilegios asignados se deberán revisar y actualizar de forma periódica por parte del grupo de infraestructura y el grupo de seguridad de la información de la Subdirección IDT.

La Subdirección de IDT y el grupo de infraestructura deberán establecer controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información de la ACNP-CCE no puedan por medio de programas de cómputo que sean instalados en sus recursos utilitarios escalar privilegios y/o evadir controles de seguridad y privacidad.

Una vez terminada la relación laboral por parte del contratista y funcionario, el grupo de infraestructura de la Subdirección IDT deberá retirar en el menor tiempo posible los derechos y privilegios de acceso a la información y a las instalaciones de procesamiento de información de la Entidad.

d) Administración y monitoreo de usuarios de altos privilegios.

El área de Infraestructura de la Subdirección de IDT otorgará los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios y contratistas designados para dichas labores, entregando cuentas personalizadas y o genéricas a cada uno de los administradores.

El área de infraestructura y el grupo de seguridad de la información de la Subdirección de IDT deberán definir las medidas de seguridad y privacidad técnicas pertinentes que permitan el monitoreo de las cuentas privilegiadas en las diferentes plataformas tecnológicas de la Entidad.

El área de infraestructura de la Subdirección de IDT deberá genera los reportes de uso de cada uno de los sistemas de información y/o recursos tecnológicos, así como deberá identificar la periodicidad de actividad o inactividad de los usuarios, con el fin de definir el periodo de inactivación que generará el bloqueo del usuario una vez validado con el área pertinente.

e) Acceso a la red inalámbrica.

Los funcionarios y contratistas de la Entidad deberán acceder a la red inalámbrica interna de la ANCP-CCE solo con los equipos autorizados.

Los funcionarios y contratistas no deberán entregar las credenciales de acceso a la red inalámbrica de la ANCP-CCE a visitantes y/o personas externas a la Entidad que no estén autorizadas.

Los funcionarios y contratistas que deseen conectar equipos a la red WIFI y que sean distintos a los equipos oficiales asignados por la Entidad, deberán conectarse únicamente a la red definida y autorizada por el grupo de infraestructura de la Subdirección de IDT.

Los visitantes a las instalaciones de la ANCP-CCE podrán ingresar libremente a la red de Visitantes de la Entidad siguiendo el proceso de registro definido por la Subdirección de IDT.

La ANCP-CCE cuenta con las siguientes redes inalámbricas: (i) La red inalámbrica a la cual solo deberá ingresar los equipos autorizados de funcionarios y contratistas de la ANCP-CCE (ii) La red inalámbrica a la cual los funcionarios y contratistas pueden hacer uso para los dispositivos personales. El acceso a esta red inalámbrica se hace mediante las credenciales personales de cada funcionario o contratista. (iii) La red inalámbrica a la cual pueden ingresar visitantes, por lo cual, deberá tener las restricciones necesarias para garantizar la Seguridad de la Información. Para poder ingresar a la red de visitantes, se deberá solicitar la contraseña por el medio indicado al grupo de infraestructura de la subdirección IDT.

f) Acceso remoto

El grupo de infraestructura de la Subdirección de IDT deberá implementar los métodos y controles técnicos de seguridad y privacidad para establecer conexiones remotas seguras a las plataformas tecnológicas y herramientas de la ANCP-CCE, permitiendo acceder únicamente al personal autorizado.

Los funcionarios y contratistas de la ANCP-CCE que realizan conexión remota, deberán contar con las aprobaciones requeridas para establecer dicha conexión y deberán tomar las medidas pertinentes para asegurar la información de la Entidad en dichas conexiones.

g) Responsabilidades de los usuarios:

Los contratistas y/o funcionarios deberán cumplir con las prácticas, lineamientos o instructivas que el grupo de infraestructura de la Subdirección IDT establezca para el uso de información y autenticación.

El grupo de Sistemas de Información de la Subdirección de IDT deberá restringir el acceso a los códigos fuente de los programas responsabilidad y/o propiedad de la Entidad.

Las contraseñas de los contratistas y funcionarios de la Entidad deberán poseer un nivel de complejidad mínimo y deberán ser cambiadas y/o actualizadas cada cierto periodo de tiempo, que deberá ser definido formalmente por el grupo de infraestructura de la Subdirección IDT.

8.4. Uso de recursos Criptográficos-Criptografía.

Objetivos: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

a) Uso de controles criptográficos:

El grupo de infraestructura de la Subdirección de IDT deberá verificar que todo sistema de Información y/o aplicativo que requiera realizar transmisión de información clasificada o reservada, utilice mecanismos de cifrado para dicha actividad.

El grupo de infraestructura y el grupo de seguridad de la información de la Subdirección de IDT establecerán los lineamientos de administración, protección y ciclo de vida de las llaves criptográficas, por medio de la implementación formal del documento que regule el uso, protección y el tiempo de vida de las llaves criptográficas. (en caso de aplicar)

La Subdirección de IDT deberá gestionar los controles criptográficos, para la protección de claves de acceso a sistema, la información reservada y/o clasificada, así como para el envío de correos electrónicos con información de la Entidad clasificada como reservada y/o clasificada. (en caso de aplicar)

8.5. Seguridad física y del entorno:

Objetivos: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones físicas de procesamiento de información de la organización, así como prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.

a) Áreas seguras-controles físicos:

La Subdirección de IDT, la Secretaria General y el área de gestión física de la Entidad deberán proveer las condiciones físicas y medioambientales necesarias para la correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo de la Entidad.

El líder de infraestructura, el Subdirector de IDT y/o quienes ellos deleguen, son los únicos responsables de autorizar el acceso de personal a los centros de cómputo de la Entidad. Se deberán llevar registro del ingreso al centro de cómputo en una bitácora ubicada en la entrada de estos lugares de forma visible.

La Subdirección de IDT y el área de gestión documental de la Entidad deberán definir y usar perímetros de seguridad, con el fin de proteger las áreas en las que se custodie que contengan información sensible o critica en los archivadores y/o lugares de gestión física de información.

La Subdirección IDT y la Secretaria General deberán definir perímetros de seguridad, con el fin de proteger las áreas que contengan información confidencial y/o critica, con el fin de evitar el ingreso de personas no autorizadas.

La Subdirección de IDT y la Secretaria General deberán diseñar e implementar mecanismos de seguridad física en las oficinas, recintos e instalaciones que tengan equipos de cómputo y/o información confidencial con el fin de protegerlos.

El grupo de seguridad y privacidad de la información de la Entidad deberá diseñar e implementar las medidas y el plan de protección física y recuperación contra desastres naturales, ataques maliciosos y/o accidentales que puedan afectar la seguridad de la información.

El grupo de infraestructura de la Subdirección IDT deberá verificar las medidas de seguridad de los activos que se encuentren fuera de las instalaciones de la Entidad.

Las salidas e ingresos de personal a las instalaciones de la ANCP-CCE, deberán ser registrados, por lo tanto, los funcionarios y contratistas deberán cumplir completamente con los controles físicos establecidos, como portar el carné y el control biométrico que sea establecido.

En caso de pérdida del carné y/o tarjeta de acceso a las instalaciones de la Entidad, los contratistas y funcionarios deberán reportarlo inmediatamente a la Secretaría General y a la Subdirección de IDT de la ANCP-CCE.

Los funcionarios y contratistas no deberán ingresar a áreas a las cuales no tengan autorización y deberán guiar a los visitantes para seguir el protocolo establecido de seguridad de ingreso de visitantes.

b) Equipos, escritorio y pantalla limpia:

Los equipos tecnológicos deberán estar ubicados y protegidos para reducir los riesgos de amenazas, los peligros del entorno y las posibilidades de acceso no autorizado.

Los equipos se deberán protegerse contra fallas de energía e interrupciones causadas por fallas en los servicios de suministro de la Entidad.

El cableado de energía eléctrica y de telecomunicaciones que porte datos o brinde soporte a los servicios de información se deberá proteger contra interceptación, interferencia o daño.

Los funcionarios y contratistas deberán velar por la seguridad en sus puestos de trabajo. Para ello, cuando dejen desatendido el puesto de trabajo deberán bloquear sus monitores o computadores, así como deberán colocar la guaya en el caso de usar equipos portátiles y no dejar documentos visibles y/o dispositivos como medios extraíbles que pongan en riesgo la Seguridad y privacidad de la Información de la Entidad.

La secretaria General y el área de Talento Humano deberá adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles, así como una política de pantalla limpia en las instalaciones de procesamiento de información.

Los funcionarios y contratistas de la Entidad no deberán dejar encendidas sus estaciones de trabajo u otros recursos tecnológicos en horas no laborables, con excepción de que se requiera un trabajo remoto.

Los equipos de cómputo, en ninguna circunstancia, deberán ser dejados desatendidos en lugares públicos o lugares que puedan afectar la seguridad.

Los equipos de cómputo deberán ser transportados con las medidas de seguridad apropiadas, que garanticen su Integridad física.

8.6 Seguridad de las operaciones.

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información, así como, asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos, pérdida de datos, aprovechamiento de vulnerabilidades, etc. con el fin de llevar registros de los eventos para asegurar la Integridad de los sistemas operacionales y minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

a) Responsabilidades:

El grupo de seguridad de la información y el grupo de infraestructura de la Subdirección IDT, deberán documentar y poner a disposición de la Entidad, los procedimientos de operación que sean requeridos.

El grupo de seguridad de la información de la Subdirección de IDT deberá controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que puedan afectar la seguridad y privacidad de la información.

El grupo de infraestructura, el grupo de operaciones y el grupo de aplicaciones de la Subdirección IDT, deberá separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

La Subdirección de IDT deberá implementar procedimientos para controlar la instalación de software en sistemas operativos.

Se deberán verificar por medio de auditorías los sistemas operativos, con el fin de minimizar las interrupciones en los procesos de negocio.

a) Copias de respaldo y seguridad:

El grupo de infraestructura de la Subdirección de IDT es el área encargada de definir y mantener los procedimientos para hacer copias de respaldo de la información, software e imágenes de los sistemas, así como, de ponerlas a prueba regularmente de acuerdo con el documento de copias de respaldo que sea formalizado para la Entidad.

Es responsabilidad de los funcionarios y contratistas de la Entidad, garantizar las copias de seguridad y respaldo de la información que resida en el equipo o recurso tecnológico asignado, siguiendo el mecanismo definido por el grupo de infraestructura de la Subdirección de IDT de la Entidad.

Al finalizar su vinculación laboral y/o contractual con la Entidad, los funcionarios y contratistas deberán entregar e informar al supervisor del contrato o jefe inmediato el lugar y acceso al repositorio de su la información que fue trabajada debido a sus obligaciones contractuales.

El grupo de infraestructura de la Subdirección de IDT deberá definir y documentar un plan o procedimiento de copias de respaldo y restauración de información.

b) Código malicioso:

Los funcionarios y contratistas de la ANCP-CCE no deberán cambiar y/o eliminar la configuración de software de seguridad y el antivirus dispuesto por la Entidad, en los equipos de cómputo y/o recursos tecnológicos que les sean asignados.

Los equipos y recursos tecnológicos (computadores portátiles, dispositivos móviles, entre otros) que sean proporcionados por la Entidad a los funcionarios y contratistas para la ejecución de sus labores, deberán contar con controles para la detección y prevención de códigos maliciosos y antivirus.

Los funcionarios y contratistas de la ANCP-CCE deberán asegurarse de abrir únicamente los archivos adjuntos que les sean enviados por correo electrónico, descargados de internet y/o copiados por cualquier medio de almacenamiento que provengan de fuentes conocidas y seguras, con el fin de evitar la propagación de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos de la Entidad.

Los funcionarios y contratistas que sospechen o detecten algún virus o software deberán notificar a la Mesa de Ayuda de forma inmediata y sin dilación, con el fin que se puedan tomar las medidas de control correspondientes.

c) Gestión de vulnerabilidades técnicas:

El grupo de seguridad y privacidad de la información de la Subdirección de IDT deberá monitorear periódicamente la posible aparición de nuevas vulnerabilidades en los sistemas de información.

El grupo de seguridad y privacidad de la información de la Subdirección IDT, deberá evaluar la exposición de la Entidad a las vulnerabilidades, con el fin de tomar las medidas apropiadas para mitigar el riesgo asociado.

El grupo de seguridad y privacidad de la información de la Subdirección de IDT, deberá ejecutar análisis de vulnerabilidades a las aplicaciones e infraestructura tecnológica crítica de la Entidad de forma periódica.

d) Registro y seguimiento de eventos:

El grupo de seguridad y privacidad de la información de la Subdirección de IDT, deberá elaborar, conservar, revisar y actualizar periódicamente los eventos de usuario (excepciones, fallas y eventos de seguridad de la información)

El grupo de infraestructura de la Subdirección IDT, deberá proteger las actividades del administrador y del operador del sistema por medio de registros, que deberán ser monitoreados con regularidad.

Los relojes de los sistemas de procesamiento de información pertinentes dentro de la Entidad se deberán sincronizar con una única fuente de referencia de tiempo.

8.7 Seguridad de las comunicaciones.

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte, así como, mantener la Seguridad de la Información transferida dentro de la organización y/o con cualquier Entidad externa**.**

a) Gestión de la seguridad de las redes:

El grupo de seguridad y privacidad de la información de la Subdirección de IDT deberá implementar los mecanismos de seguridad que considere pertinentes en la configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Entidad.

La Subdirección de IDT deberá identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red internos y externos.

El grupo de infraestructura de la Subdirección de IDT deberá segregar la red teniendo en cuenta la información, los usuarios y las plataformas tecnológicas y acogiendo las buenas prácticas de configuración que considere pertinentes.

El grupo de infraestructura de la Subdirección de IDT establecerá e implementará los controles de acceso y tráfico a las redes y subredes con el fin de mejorar su rendimiento y seguridad.

El grupo de infraestructura de la Subdirección de IDT deberá garantizar que la red para visitantes esté aislada de la red corporativa.

c) Transferencia de información:

Los funcionarios y contratistas que necesiten realizar y/o hacer envío de Información Confidencial fuera del ámbito interno e infraestructura tecnológica de la ACNP-CCE a terceros, deberán cifrar el contenido y la información, con el propósito de proteger su Confidencialidad e Integridad.

El grupo de infraestructura de la Subdirección de IDT definirá, documentará y compartirá los procedimientos adecuados de intercambio de información entre las plataformas de la ACNP-CCE con los sistemas de terceros.

El grupo de seguridad y privacidad de la información deberá identificar, revisar y documenta los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Entidad en la protección de la información.

d) Uso de correo electrónico corporativo:

Los funcionarios y contratistas de la ANCP-CCE no deberán en ninguna circunstancia utilizar y/o acceder a una cuenta de correo institucional que no sea la propia, los buzones de correo de la cuenta que sea asignada a cada funcionario son propiedad de la Entidad y cada usuario, como responsable de su buzón, deberá mantener solamente los mensajes relacionados con el desarrollo de sus labores.

Los funcionarios y contratistas no deberán enviar archivos adjuntos que contengan extensiones ejecutables, en ninguna circunstancia y/o sin la autorización requerida.

La Subdirección IDT y Secretaría General deberán identificar, revisar y documentar los acuerdos de confidencialidad y no divulgación que reflejen las necesidades de la organización para la protección y seguridad de la información y de los datos personales.

8.8. Adquisición, desarrollo y mantenimiento de sistemas.

Objetivo: Asegurar que la Seguridad de la Información sea una parte integral de los sistemas de información durante todo el ciclo de vida de desarrollo de los sistemas de información.

a) Seguridad de los sistemas d información:

El grupo de sistemas y el grupo de infraestructura de la Subdirección de IDT, deberán proteger la información que sea involucrada en las transacciones de servicios de las aplicaciones, con el fin de evitar transmisión incompleta, enrutamiento errado, alteración, divulgación, duplicación y/o reproducción no autorizada de mensajes.

El grupo de sistemas y el grupo de infraestructura de la Subdirección de IDT, deberán proteger la información de los servicios de las aplicaciones sobre redes públicas contra actividades fraudulentas, disputas, divulgación y modificación no autorizadas.

La Subdirección de IDT deberá considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los sistemas de información, pasando desde el diseño hasta la puesta en marcha.

b) Seguridad en los procesos de desarrollo y soporte:

El grupo de sistemas de información de la Subdirección de IDT deberá implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

El grupo de sistemas de información de la Subdirección de IDT deberá contar con sistemas de control dentro del ciclo de vida de desarrollo de versiones para administrar los cambios de los sistemas de información en la Entidad.

El grupo de sistemas y el grupo de infraestructura de la Subdirección de IDT deberá generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

Los desarrolladores y gestores de las aplicaciones de terceros deberán documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera de acuerdo con los requerimientos de seguridad establecidos y los controles deseados.

Los desarrolladores y gestores de aplicaciones de terceros deberán deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible, así como, deberán establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo y certificar la transmisión de Información Confidencial por medio de canales seguros.

Los desarrolladores y gestores de aplicaciones de terceros deberán asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los desarrolladores y gestores de aplicaciones de terceros deberán suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deberán encontrarse disponibles en todas las páginas protegidas por autenticación.

Los desarrolladores y gestores de aplicaciones de terceros deberán garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deberán implementar mensajes de error genéricos.

Los desarrolladores deberán remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción y deberán prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Los desarrolladores deberán remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
Los desarrolladores deberán evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deberán estar en archivos de configuración independientes, los cuales deberían estar cifrados.

Los desarrolladores deberán certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas y deberán proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Los desarrolladores deberán asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo y deberán cumplir con los demás lineamientos establecidos y buenas prácticas que se hayan adoptado por la Entidad.

8.9. Relaciones con los proveedores.

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores**.**

a) Seguridad de la información en relaciones con proveedores:

La Secretaría General y la Subdirección IDT deberá definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la ANCP-CCE y terceras partes, dichos acuerdos deberán incluir los requisitos de seguridad de la información para procesar, almacenar, comunicar y suministrar los servicios de TI para la Entidad.

La Secretaria General y la Subdirección IDT deberán definir en los acuerdos de confidencialidad los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios asociados a tecnologías de la información, se deberá regular la prohibición de los proveedores a la divulgación de la información entregada por la ANCP-CCE a terceros no autorizados, así como, se deberán establecer la destrucción de dicha información una vez cumpla su cometido, de acuerdo con los requisitos asociados al tratamiento de la información, seguridad y privacidad.

Los propietarios de los Activos de Información deberán verificar el cumplimiento de los Acuerdos de Confidencialidad y/o Acuerdos de intercambio establecidos con los proveedores.

Los propietarios de los Activos de Información o a quien ellos deleguen, deberán verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

Los propietarios de los Activos de Información deberán hacer seguimiento a la prestación de los servicios de los proveedores.

La Subdirección IDT deberá documentar e implementar un lineamiento de seguridad de la información para las relaciones con terceros, con el fin de mitigar los riesgos asociados con el acceso de proveedores a los activos de información de la Entidad.

8. 10. Gestión de Incidentes de Seguridad de la Información.

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de Seguridad de la Información, incluida la comunicación sobre eventos de seguridad y sus debilidades.

a) Conducta, responsabilidades y restricciones:

La Subdirección IDT deberá brindar los recursos necesarios establecer las responsabilidades y procedimientos para la gestión efectiva, rápida y eficaz de los incidentes de seguridad de la información.

El grupo de seguridad y privacidad de la información de la Subdirección de IDT, deberá evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares a través de los canales establecidos en el menor tiempo posible.

Los propietarios de los Activos de Información, los contratistas y funcionarios deberán informar a la Subdirección IDT en el menor tiempo posible, cualquier incidente de seguridad de la información que identifiquen o que reconozcan, sin importar su posibilidad de materialización y por el medio definido por la Entidad que es el canal de Mesa de Ayuda.

En caso de conocer la pérdida o divulgación no autorizada de información definida como confidencial, clasificada o reservada y/o datos personales sensibles, los funcionarios y contratistas deberán notificarlo a los propietarios de los activos y el Grupo de Seguridad y Privacidad de la información de la Subdirección IDT.

El grupo de seguridad de la información de la Subdirección de IDT deberá documentar y evaluar los incidentes de seguridad de la información con el fin de aplicar oportunidades de mejora y reducir la posibilidad o impacto de incidentes futuros.

8. 11. Gestión de continuidad de negocio.

Objetivo: incluir la continuidad de Seguridad de la Información en los sistemas de gestión de la continuidad de negocio de la Entidad y asegurar la disponibilidad de instalaciones de procesamiento de información.

a) Continuidad de la seguridad de la información:

La Subdirección IDT es la encargada de determinar los requisitos para la seguridad de la información y la continuidad de la gestión del negocio en situaciones adversas como emergencias, desastres y/o ataques, los dueños de los procesos y/o cada una de las áreas de la Entidad deberán determinar cómo se deberá actuar frente a una situación adversa para la seguridad de la información que afecte la continuidad del negocio con el fin de generar el Plan de Continuidad adecuado.

La Subdirección de IDT deberá aprobar un plan de recuperación ante desastres para los casos que considere necesario y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para los servicios y Sistemas de Información que se incluyan.

La Subdirección IDT deberá verificar de forma periódica los controles de continuidad de la seguridad de la información establecidos e implementados con el fin de asegurar y documentar su eficacia durante las situaciones adversas.

Los Dueños de procesos deberán generar la documentación necesaria que podrá ser utilizada en caso de un evento adverso, teniendo en cuenta la Seguridad de la Información. Estos documentos deberán ser evaluados por el grupo de seguridad de la información y grupo de infraestructura de la Subdirección IDT para garantizar su efectividad.

La Subdirección de IDT deberá analizar y establecer los requerimientos de redundancia suficientes para los sistemas e instalaciones de procesamiento de información críticos que determine la Entidad y cumplir con los requisitos de disponibilidad.

La Subdirección de IDT deberá evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Entidad.

8.12. Cumplimiento.

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias y/o contractuales, relacionadas con Seguridad de la Información y de cualquier requisito de seguridad con el fin de asegurar que la Seguridad de la Información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

a) Conducta, responsabilidades y restricciones:

La Secretaria General deberá proyectar, documentar y actualizar, cuando sea necesario, el normograma que se deberá incluir y cumplir con las regulaciones vigentes y aplicables en temas de Seguridad y privacidad de la información.

Los funcionarios y contratistas deberán cumplir con todos requisitos estatutarios, regulatorios, contractuales relacionados con la seguridad de la información y de cualquier requisito de seguridad.

La Secretaría General deberá socializar a los funcionarios y contratistas con el deberá de cumplimiento de las leyes de derechos de autor, con el fin de evitar duplicar contenido y/o software sin la autorización del propietario de los derechos de autor. La reproducción no autorizada es una violación de Ley; no obstante, dependiendo de la licencia otorgada, se puede permitir su uso, copia o reproducción bajo escenarios específicos.

El grupo de infraestructura de la Subdirección IDT deberá usar controles criptográficos (en caso de aplicar) en cumplimiento de todos los acuerdos legales y reglamentarios pertinentes.

El grupo de seguridad de la información de la Subdirección IDT deberá revisar los sistemas de información de forma periódicamente para determinar el cumplimiento con las Políticas y normas de seguridad de la información.

b) Privacidad en Datos Personales:

El grupo de seguridad y privacidad de la información de la Subdirección IDT y la Secretaria General de la Entidad deberán implementar los controles de seguridad de la información para el tratamiento y protección de los datos personales de los funcionarios y contratistas de la ANCP-CCE.

El oficial de datos personales de la Entidad y/o quien haga sus veces, deberá velar por la implementación efectiva de las Políticas y procedimientos para el tratamiento de datos personales en la Entidad con el fin de cumplir con sus obligaciones y las regulaciones aplicables.

El oficial de datos personales de la Entidad y/o quien haga sus veces, deberá velar por la implementación de buenas prácticas para la gestión y tratamiento de los datos personales dentro de la Entidad, con el fin de (i) estructurar, diseñar y administrar el programa y/o sistema de protección de datos personales y, (ii) establecer el monitoreo y controles sobre el programa y/o sistemas de datos personales, su evaluación y revisión periódica.

El oficial de datos personales de la Entidad y/o quien haga sus veces, es un rol diferente a el oficial de seguridad de la información, el de datos deberá tener conocimientos de la aplicación y cumplimiento de la legislación de datos personales aplicable y vigente.

El oficial de datos personales de la Entidad y/o quien haga sus veces será el encargado de coordinar con todas las áreas de la Entidad la definición e implementación de los controles del programa y/o sistema de datos personales, así como, será el encargado de servir de enlace con las áreas con el fin de asegurar una implementación transversal del programa.

Deberá mantenerse un inventario de las bases de datos personales de la Entidad, y deberán ser registradas periódicamente y/o cuando existan cambios sustanciales en el Registro Nacional de Bases de Datos de la Entidad atendiendo las instrucciones emitidas por la SIC. Son los dueños de los activos de información los responsables de reportar las bases de datos que tengan a su disposición y7o tratamiento al oficial de datos personales de la Entidad y/o quien haga sus veces.

Los funcionarios y contratistas de la Entidad deberán recibir capacitación sobre el régimen de protección de datos personales por parte del grupo de seguridad y privacidad de la información de la Subdirección IDT.

Los funcionarios y contratistas de la ACNP-CCE deberán aceptar y conocer la Política de Tratamiento de Datos Personales de la Entidad.

La Subdirección de IDT deberá implantar los controles necesarios para proteger la información personal de funcionarios, contratistas, proveedores u otras terceras partes, que es almacenada en las plataformas del SECOP y/o en las bases de datos o cualquier otro repositorio de la Entidad, con el fin de evitar su divulgación, alteración y/o eliminación.

Los funcionarios y contratistas que tengan bajo su custodia información que contenga datos personales deberán asegurar que a dicha información solo tendrán acceso aquellas personas autorizadas que tengan una necesidad legítima, así como, deberán acogerse a las directrices técnicas y procedimientos establecidos para el intercambio de estos datos.

Las plataformas y/o herramientas de la Entidad que recolecten y traten datos personales, deberán cumplir con las obligaciones establecidas en las regulaciones aplicables para la protección de la información personal.

8.13 Almacenamiento de información y Backups de usuario.

Objetivo: garantizar que la información y la infraestructura de la Entidad, sean respaldadas y que puedan ser restauradas en caso de una falla y/o desastre.

El área de infraestructura de la Subdirección IDT deberá validar que el disco duro que sea instalado en los equipos asignados a los funcionarios y/o contratistas respectivamente deberá tener una capacidad de almacenamiento entre 500 Gigabytes 1 Terabyte dependiendo del tipo de equipo asignado.

Los funcionarios y/o contratistas de la ANCP-CCE deberán utilizar sus equipos y el espacio de uso, cumpliendo con las obligaciones legales que les sean aplicables y respetando los derechos de autor, la información que sea consignada en c/u de los equipos es responsabilidad del funcionario y contratista.

Los funcionarios y/o contratistas de la ANCP-CCE, tendrán a su disposición el disco de internet (OneDrive), que es el servicio de almacenamiento que presta Microsoft, como parte de la suscripción de Colombia Compra Eficiente a las licencias de Office 365. El OneDrive tiene una capacidad de 1 Terabyte para cada funcionario o contratista que tenga una cuenta de Office 365 asignada.

Los funcionarios y/o contratistas de la ANCP-CCE son responsables de tener, organizar y guardar la información laboral en los espacios de almacenamientos oficiales de la Entidad. En este caso el espacio de almacenamiento en la nube garantiza la Disponibilidad y la Integridad ante cualquier borrado por parte del usuario, el usuario puede recuperar la información y/o solicitar ayuda a la Mesa de Ayuda para recuperar su información.

Los Subdirectores y/o la persona que sea definida de cada dependencia de la ANCP-CCE se encargarán de la creación y/o eliminación de los espacios colaborativos en el servidor de nube, especificando el grupo de personas que podrán tener acceso. En este espacio los funcionarios y contratistas podrán trabajar con las personas asignadas la información asociada al objetivo de cada carpeta.

El grupo de infraestructura de la Subdirección IDT, deberá crear y proyectar el documento que regule la periodicidad y la manera de hacer backups en la ANCP-CCE.

8.14. Archivo Electrónico de Gestión Documental.

Objetivo: Adoptar las medidas necesarias para garantizar la integridad física y funcional de los documentos

La Secretaría General y el área de Gestión Documental de la ANCP-CCE, deberán definir e implementar las estrategias de conservación y preservación digital a largo plazo con el fin de garantizar la documentación electrónica de la Entidad, siguiendo los lineamientos y estructura de las Tablas de Retención Documental.

El archivo digital de la Entidad será guardado en la plataforma -SharePoint- aquella que la reemplace y/o aquella que sea asignada en una carpeta para cada proceso de la Entidad. Cada carpeta contará con un responsable asignado por el Director, Secretario General y/o Subdirector de su respectiva dependencia, quien se encargará de gestionar el manejo de este espacio, el cargue de los documentos, los permisos necesarios que requiera y validar que la información en su carpeta este completa, terminada y acorde a los lineamientos definidos por el área de Gestión Documental.

Para la gestión de los permisos, el responsable de la carpeta podrá solicitar los permisos por medio de la plataforma de Mesa de Ayuda, los cuales serán revisados por el grupo de infraestructura y seguridad de la información de la Subdirección IDT, para ser posteriormente aprobados y/o rechazados.

8. 15. Lineamientos para el mantenimiento de los centros de cómputo

Objetivo: Con el fin de prevenir y mitigar cualquier riesgo de seguridad relacionado con los cuartos técnicos, la ANCP-CCE define los siguientes lineamientos.

El área de soporte e infraestructura de la Subdirección de IDT, deberá velará porque el cableado de red dentro de este protegido contra daños y/o accesos no autorizados, evitando la exposición de dispositivos. de red en áreas de acceso público.

Con el fin de evitar la interferencia, los cables de energía y de datos, deberán estar separados entre sí.

Los espacios físicos y/o los lugares dónde se encuentren los centros de cómputo de la ANCP-CCE deberán asegurarse con las medidas adecuadas de seguridad física. La puerta de salida deberá encontrarse libre de obstrucciones en todo momento.

Antes de autorizar a un empleado para ingresar al centro de cómputo, ya sea temporalmente o no, se deberá diligenciar el formato de autorización para dar ingreso al centro de cómputo por medio de la creación del caso en GLPI.

Son responsabilidades de los funcionarios y contratistas autorizados a entrar a los centros de cómputo seguir las reglas acerca del no ingreso de alimentos, bebidas y/o el consumo de cigarrillo dentro de los centros de cómputo de la Entidad

Los residuos deberán arrojarse siempre en cestos, los cuales deberán vaciarse periódicamente. No se deberá permitir que los residuos se apilen en el piso o sobre los equipos.

Los líquidos inflamables (incluyendo productos de limpieza) deberán permanecer fuera del centro de cómputo: (i) todo personal de limpieza que acceda al centro de cómputo deberá encontrarse autorizado para acceder a éste. (ii) La temperatura en el centro de cómputo deberá mantenerse a un nivel adecuado. entre 18 y 22 grados Celsius con una humedad relativa del 50%. (iii) Se deberá tener un registro de todos los dispositivos que ingresen y salgan del centro de cómputo, así como su responsable. (v) Los centros de cómputo deberán estar equipados con sensores de humedad y temperatura, los cuales deberán ser probados periódicamente. (vi) Mantener un inventario de todas las llaves y guardarlas en un lugar seguro.

8.16. Lineamientos para el cifrado de la información.

Los funcionarios y contratistas de la ANCP-CCE deberán cifrar la Información confidencial y critica cuando las circunstancias lo exijan. El cifrado de la información se puede realizar con diversas herramientas y algoritmos: (i) Cifrado con 7-zip (ii) Protección con Office. Para más información se puede consultar a la Mesa de Ayuda y/o al grupo de infraestructura de la Subdirección IDT.

El área de infraestructura de la subdirección IDT deberá elaborar un instructivo que contenga los puntos específicos para el cifrado de la información.

VIGENCIA DEL MANUAL

El presente Manual entra en vigor a partir del momento de su publicación y divulgación y se entiende vigente de manera indefinida a menos que se modifique para actualizarlo. Las revisiones, actualizaciones (cuando apliquen) del presente Manual deberán ser realizadas de manera periódica por el grupo de seguridad y privacidad de la información de la Subdirección IDT.

INSTRUCTIVOS RELACIONADOS.

1. Instructivo para la Gestión de usuarios y contraseñas.
2. Instructivo para el Ingreso Seguro a los Sistemas de Información.
3. Instructivo para Códigos Maliciosos
4. Instructivo para la Gestión de Capacidad.
5. Instructivo para la Separación de Ambientes
6. Instructivo para la Gestión de Activos
7. Instructivo para la Gestión de Incidentes de Seguridad y Privacidad de la Información.
8. Instructivo para la Transferencia de Información.

ANEXOS.

- Inventario de Activos de Información.
- Matriz de Riesgos de Seguridad de la Información.
- Guía de Roles y Responsabilidades: Seguridad y Privacidad de la Información.
- Plan de Comunicación, Sensibilización y Capacitación.

FICHA TÉCNICA DE DOCUMENTO Y CONTROL DE CAMBIOS

I. IDENTIFICACIÓN Y UBICACIÓN DEL DOCUMENTO								
Título:	Manual de Seguridad y Privacidad de la Información							
Fecha de elaboración:	21	Agosto	2020	**Fecha de aprobación:**	22	Diciembre	2020	
Resumen de contenido:	El Manual de Seguridad y Privacidad de la Información de la ANC-CCE define los lineamientos para la adecuada gestión de la seguridad y privacidad de los Activos de Información en la Entidad, con de protegerlos contra la pérdida de Confidencialidad, Integridad, Disponibilidad y/o Privacidad forma accidental o intencionada, especificando las medidas organizacionales, técnicas y físicas fueron definidas en la Política de Seguridad y Privacidad de la Información y en cumplimiento normatividad vigente y aplicable.							
Área / Dependencia:	Subdirección de Información y Desarrollo Tecnológico							
Código:	CCE-SGI-GI-02			**Estado:**	Aprobado			
Categoría - Tipo de documento	IDI							
Autor / Autores:	Ana María Cárdenas							
Aprobación por: **Cargo:**	Rigoberto Rodríguez Peralta							
Nombre:	Subdirector de Información y Desarrollo Tecnológico							
Información adicional:								
Tipo de documento: (Marque X)	Físico		( )	Electrónico	(X)			
Ubicación: (especifique donde se aloja o reposa el documento)								

I. AUTORIZACIONES RESPONSABLES						
Acción	**Nombre**	**Cargo / Perfil**	**Fecha**			**Firma**
Elaboró Jurídicamente	Ana María Cárdenas	Contratista Subdirección de Información y Desarrollo Tecnológico	21	Agosto	2020	Ana Maria Cardenas
Revisó Técnicamente	Milena Cabrales	Contratista Líder de Seguridad de la Información	16	Octubre	2020	Milena Cabrales
Revisó y aprobó	Rigoberto Rodríguez Peralta	Subdirector de Información y Desarrollo Tecnológico	22	Octubre	2020	Rigoberto Rodríguez Peralta
Aprobó	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	22	Diciembre	2020	Acta 22 de diciembre del 2020
¿Aprobación mediante comité interno? A continuación, Marque **X** en **SI** o **NO**						**SI** X **NO**
Nombre de comité interno:	Comité Institucional de Gestión y Desempeño					
Acto administrativo de conformación comité interno:						
Fecha de conformación de comité interno:						
Medio de Aprobación de este documento:						

Nota1: Si ha marcado (**NO**) **en la sección de: "¿Aprobación mediante comité interno?"** marque N/A (No aplica) en los siguientes 4 espacios de preguntas correspondientes a la sección de autorizaciones responsables.

Nota2: Diligenciar las fechas de la siguiente manera Dia: diligenciar dos dígitos en números; Mes: diligenciar el mes con las tres primeras letras del mes, ejemplo: Ene = Enero, Ago = Ago. Año: Diligenciar el año con los cuatro dígitos.

I. CONTROL DE CAMBIOS DE DOCUMENTO			Versión vigente del documento:		03
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
No. 1	12/12/2016	Creación del documento	Santiago Carvajal Torres	María Margarita Zuleta González	Comité Directivo e Institucional de Desarrollo Administrativo de Colombia Compra Eficiente
No. 2	19/07/2018	Actualización del documento	Luis Alejandro Ruiz	Dana Pineda Marín	Comité Institucional de Gestión y Desempeño
No. 3	22/12/2020	Actualización del documento	Milena Cabrales Contratista Líder de Seguridad	Rigoberto Rodríguez subdirector de IDT	Comité Institucional de Gestión y Desempeño

_____

Nota: El control de cambios en el documento, se refiere a cualquier ajuste que se efectúe sobre el documento que describe ficha técnica del presente documento.