Agencia Nacional
de Contratación Pública
Colombia Compra Eficiente

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA - COLOMBIA COMPRA EFICIENTE – 2024

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. JUSTIFICACIÓN

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (en adelante, ANCP-CCE) identifica la seguridad y Privacidad de la información como un componente indispensable para alcanzar los objetivos definidos en el Plan Estratégico de la Agencia, reconoce la importancia de la información que gestiona y la vela por la adecuada protección de sus activos de información, por lo tanto, se compromete a implementar un Sistema de Gestión de Seguridad de la Información conforme al Modelo de Seguridad y Privacidad de la Información (en adelante el MSPI) de esta manera se da cumplimiento a las recomendaciones y lineamientos establecidos desde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), dando cumplimiento a lo establecido en las políticas de gobierno digital con el propósito de realizar el aseguramiento que permita proteger la Integridad, Confidencialidad, la Disponibilidad, Privacidad y No repudio de la información que gestiona en el ejercicio de sus operaciones y en concordancia con el objeto misional de la Entidad.

2. OBJETIVO GENERAL

Establecer las directrices, lineamientos y las medidas organizacionales de seguridad que permitan proteger, asegurar y fortalecer la adecuada gestión de la seguridad y privacidad de la información de la ANCP-CCE; enmarcadas en la implementación del Modelo de Seguridad y Privacidad de la Información (en adelante, MSPI) que ha sido definido por Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y alineado a la política de gobierno digital, dentro del Sistema de Gestión de Seguridad de la Información (En adelante SGSI) de la entidad, con el fin de evitar, prevenir y mitigar los riesgos que comprometan los principios de seguridad de la información.

2.1 OBJETIVOS ESPECIFICOS

- Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y continuidad de la operación de los servicios de la entidad.

- Mitigar el impacto de los incidentes de seguridad, y privacidad de la información de forma efectiva, eficaz y eficiente.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la Confidencialidad, Integridad, Disponibilidad, Autenticidad, Privacidad y no repudio de la información de la ANCP-CCE.
- Generar un cambio organizacional a través de la concientización y apropiación de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información de la entidad.
- Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información vigentes y aplicables.
- Definir, operar y mantener el Plan de Continuidad del Negocio para las Plataformas de la ANCP-CCE.

3. ALCANCE

Hace parte del alcance de esta Política, toda la información creada, procesada, tratada 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.

Lo establecido en el presente documento, anexos y/o posteriores actualizaciones es aplicable y de obligatorio cumplimiento para:

a. 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.

b. Las Entidades de control y demás entidades relacionadas que accedan, a cualquier Activo de Información propiedad de la ANCP-CCE, independientemente de su ubicación.

c. Los procesos y áreas internas que traten Activos de información en cumplimiento de sus objetivos estratégicos.

4. DEFINICIONES

- **Activo de Información**: Es toda aquella información o elemento que reside en medio digital o físico, que tiene un significado y valor para la entidad, y por ende necesita ser protegido.
- **Algoritmo de Cifrado**: Secuencia de instrucciones matemáticas usadas para transformar textos o datos legibles y entendibles en textos o datos cifrados y viceversa.
- **Aplicación Endpoint**: Software cuya función es detectar y/o eliminar aplicaciones maliciosas informáticas.
- **Ambiente**: conjunto de elementos o componentes tecnológicos o, grupos de sistemas de información, en los cuales reside o fluye información y datos de negocio.
- **Backup**: Se refiere a la copia de seguridad de los datos realizada en un dispositivo de almacenamiento (disco duro externo, entre otros). Al hacer un backup, se crea una copia de seguridad de los datos a partir de la cual se pueden restaurar posteriormente en caso de pérdida.
- **Cifrado**: Proceso sistemático que convierte la información legible en formato ilegible mediante la utilización de algoritmos matemáticos y llaves criptográficas. El cifrado se utiliza para proteger la información de la divulgación no autorizada.
- **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.
- **Confidencialidad**: Es el principio de la Seguridad de la Información que busca asegurar que la información de la entidad sea accedida o revelada únicamente por el personal autorizado.
- **Componentes de Infraestructura Tecnológica**: hace referencia a los elementos necesarios para operar y gestionar entornos de TI empresariales. Estos elementos incluyen el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos, entre otros.

- **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.
- **Custodia Física o Digital**: Es la acción de proteger la información teniendo cuenta los principios de confidencialidad, integridad y disponibilidad.
- **Dato Personal**: Información que identifique o permita identificar a una persona natural.
- **Disponibilidad**: Es el principio de la Seguridad de la Información que busca asegurar que la información de la entidad 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.
- **Integridad**: Es el principio de la Seguridad de información que busca garantizar que la información no pueda ser adulterada o modificada por un tercero no autorizado.

- **Información Confidencial**: Es la información de uso exclusivo por parte de usuarios claramente identificados y autorizados dentro de la entidad.
- **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 administrativas que se realicen o ejecuten sobre los componentes o aplicaciones de la infraestructura tecnológica generando una traza de eventos auditables.
- **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, 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.
- **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.

- **Plan de Seguridad y Privacidad de la Información (PSPI)**: Comprende todas aquellas actividades que contribuyen a la protección de la información.
- **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
- **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.
- **Seguridad de la información**: Es el conjunto de medidas que busca preservar la Confidencialidad, Integridad y Disponibilidad de la información.
- **Sistemas de Información**: Conjunto de componentes tecnológicos tales como bases de datos, servidores de aplicaciones, dispositivos de red, datos y personas que permiten el almacenamiento, transmisión y procesamiento de la información.
- **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**: Debilidad en un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

5. BASE LEGAL

La base legal de las políticas de seguridad y privacidad de la información se fundamenta en el marco jurídico que regula el adecuado manejo, protección y tratamiento de los datos personales e institucionales. Estas políticas establecen las directrices necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información, promoviendo un entorno seguro y alineado con las disposiciones legales aplicables.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MARCO NORMATIVO EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 1 base legal de la Política de TI

Identificación de la norma, ley, decreto	Descripción	Página web
Normograma de la Agencia Nacional de Contratación Pública Colombia Compra Eficiente	Normograma de la Agencia Nacional de Contratación Pública Colombia Compra Eficiente – normas aplicables en la materia	https://www.colombiacompra.gov.co/transparencia/normas-generales-y-reglamentarias-politicas-lineamientos-o-manuales-las-metas-y-objetivos-de
Constitución Política de Colombia	Artículo 15	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4125
Ley 594 de 2000	Por medio de la cual se expide la Ley General de Archivos.	https://normativa.archivogeneral.gov.co/ley-594-de-2000/
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado-denominado "de la protección de la información y de los datos"	https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

Decreto 4170 de 2011	Por el cual se crea la Agencia Nacional de Contratación Pública Colombia Compra Eficiente ANCP-CCE, se determinan sus objetivos y estructura.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44643
Decreto 1083 de 2015	Único Reglamentario del Sector Función Pública y las modificaciones introducidas al Decreto Único Reglamentario del Sector de Función Pública a partir de la fecha de su expedición.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62866
Decreto 1074 de 2015	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608
Decreto 1078 de 2015	Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888
Decreto 1008 de 2018	Lineamientos generales de la Política de Gobierno Digital, subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902
Conpes 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf
Conpes 3854 de 2016	Política Nacional de Seguridad Digital.	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
Decreto 338 de 2022	Mediante el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital, Resolución 500 de 2021- Por medio del cual se establecen los lineamientos generales, estrategias y gestión de riesgos de seguridad de la información en los procesos digitales.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
Guía-Modelo de Privacidad y Seguridad de la Información MSPI	MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

	sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar)	
Guía -Modelo de Gestión de Riesgos de Seguridad Digital	Este documento complementa y profundiza lo expuesto en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas, emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237907_maestro_mspi.pdf
NTC-ISO/ICE 27001 y NTC-ISO/ICE 27002	Para la gestión de la privacidad de la información.	https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf
ISO 22301:2019	Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.	ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements

Fuente: Elaboración propia.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6. ESTANDARES, POLÍTICAS Y PROCESOS RELACIONADO

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS CON SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 2 Identificación de estándares, políticas y procesos relacionados a la Política TI

Identificación del documento	Descripción	Página web
G.ES.03 Guía del dominio de Estrategia: Definición y diseño de una política de TI Guía técnica	Documento de Min Tic, donde se propone la estructura que deben llevar las políticas de TI	MSPI (mintic.gov.co)
Guía 3 - Procedimiento de Seguridad de la Información	Indicar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información para las entidades del estado	MSPI (mintic.gov.co)
Guía 4 - Roles y responsabilidades	Guía para la definición del equipo responsable de seguridad y privacidad de información dentro de las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.	MSPI (mintic.gov.co)

Fuente: Elaboración propia

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Identificación del documento	Descripción	Página web
Guía 5 - Gestión Clasificación de Activos	Entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del estado	MSPI (mintic.gov.co)
Guía 7 - Gestión de Riesgos	Orienta a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.	MSPI (mintic.gov.co)
Guía 8 - Controles de Seguridad de la Información	El documento presenta los objetivos de control del estándar ISO 27002	MSPI (mintic.gov.co)
Guía 10 - Continuidad de Negocio	Este documento indica la implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.	MSPI (mintic.gov.co)
Guía 12 - Seguridad en la Nube	Este documento, presenta los lineamientos y aspectos a tener en cuenta para el aseguramiento de la información en la nube	MSPI (mintic.gov.co)
Guía 17 - Mejora continua	En este documento se explica la fase final del modelo que corresponde a la mejora continua del proceso de gestión la cual pretende apoyar el mantenimiento y mejora del sistema.	MSPI (mintic.gov.co)
ISO 27001 gestión de la seguridad de la información	Esta norma nos aportan un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la continuidad de las actividades de la empresa	https://www.normas-iso.com/iso-27001/

Fuente: Elaboración propia

7. ROLES Y RESPONSABILIDADES

Con el fin de proteger los Activos de Información de cualquier pérdida de Confidencialidad, Integridad y/o Disponibilidad de forma accidental y/o intencionada, la ANCP-CCE ha establecido los siguientes principios fundamentales que soportan la implementación de la presente Política:

La ANCP-CCE, asegurará la protección de la información generada, procesada y/o resguardada por los procesos de negocio y su infraestructura tecnológica, buscando mantener la Disponibilidad, Integridad y Confidencialidad de esta.

La ANCP-CCE protegerá la información por medio de la identificación de los Activos de Información y la gestión de riesgos de Seguridad de la Información, con el objetivo de: (i) minimizar las fallas en los Sistemas de Información de Compra y Contratación Pública, (ii) minimizar el impacto de las fallas que generen indisponibilidad de la información, (iii) incrementar la satisfacción de los partícipes de la Compra y la Contratación Pública y. (iv) asegurar el cumplimiento de las obligaciones legales y regulatorias que sean aplicables.

La ANCP-CCE garantizará la gestión de los procesos para la continuidad del negocio con el fin de enfrentar los Incidentes de Seguridad y Privacidad de la Información potencialmente desastrosos para la entidad y garantizar los tiempos de respuesta que se requiere en el Sistema de Compra Pública.

La ACNP-CCE cree en la importancia de desarrollar un Sistema de Gestión de Seguridad de la Información y una cultura organizacional que le permita gestionar de manera eficiente y segura la información de la entidad.

La ACNP-CCE, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información-MSPI, enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la Confidencialidad, Integridad, Disponibilidad, Autenticidad, Privacidad y No Repudio de la información que es identificada en el mapa de procesos de la entidad y en concordancia con los siguientes lineamientos generales:

- La ANCP-CCE dirigirá de manera integral la gestión y la implementación de controles físicos y digitales con el fin de mitigar los riesgos derivados de las acciones contra los activos de información de la entidad, así mismo, implementará las medidas necesarias para para preservar la

Confidencialidad, Integridad, Disponibilidad, Privacidad y No repudio de la información dando cumplimiento a las obligaciones legales, regulatorias y contractuales vigentes, aplicables y establecidas, orientados a la mejora continua y al alto desempeño del SGSI dentro de la entidad.

- La ACNP- CCE protegerá la información contra el acceso no autorizado, con el fin de mantener su Confidencialidad, Integridad y Disponibilidad, estableciendo niveles de requerimientos de protección que serán administrados y controlados de acuerdo con la naturaleza y uso de la información.

- La información de la ANCP-CCE deberá ser clasificada por el dueño del proceso, para establecer su nivel de sensibilidad, criticidad y reserva de esta, con el fin de determinar las medidas de seguridad adecuadas en cada nivel identificado. Es responsabilidad de cada uno de los dueños de los procesos que manejan información de la entidad, como de los contratistas y terceros conocer los lineamientos de clasificación de la información que maneja la ANCP-CCE.

- La ANCP-CCE definirá, implementará, operará y mejorará de forma continua su Sistema de Gestión de Seguridad de la Información, de acuerdo con las necesidades del negocio y los requerimientos regulatorios y de cumplimiento que le sean aplicables.

- Las responsabilidades frente a la seguridad de la información serán definidas, comunicadas y publicadas por el grupo de seguridad y privacidad de la información de la ANCP-CCE y deberán ser aceptadas por cada uno de los empleados, contratistas y/o terceros de la entidad.

- La ANCP-CCE protegerá la información generada, creada, procesada, transmitida y resguardada por sus procesos de negocio y la infraestructura de la entidad, con el fin de minimizar impactos financieros, operativos y legales, debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La ANCP-CCE protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos implementando las medidas adecuadas para este fin.

- La ANCP-CCE controlará la operación de sus procesos de negocio garantizando mecanismos de seguridad en los recursos tecnológicos y las redes de datos.

- La ANCP-CCE implementará control de acceso a la información, sistemas y recursos de red.

- La ANCP-CCE garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad y privacidad.

- La ANCP-CCE garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- La ANCP-CCE garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

A continuación, se establecen las siguientes Políticas de seguridad específicas que soportan el Sistema de Gestión de Seguridad de la Información SGSI de la ANCP-CCE:

a) Política de Roles y Responsabilidades para la Seguridad y Privacidad de la Información

Esta Política, reconoce que la responsabilidad final de los activos de información de la ANCP-CCE está en quienes los "poseen" y "utilizan". Por lo tanto, la responsabilidad de asegurar la Confidencialidad, Integridad y Disponibilidad de la información depende de cada una de las personas o áreas que utilizan, supervisan y administran los sistemas de la ANCP-CCE que manejan información que reside en su infraestructura, plataformas y equipos.

Por esta razón, la entidad define 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, siguiendo los siguientes lineamientos:

Responsabilidades Alta Dirección

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

Responsabilidades del(os) Dueños de Procesos 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 y la evaluación de 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, 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.

- Realizar una evaluación anual de riesgos con el fin de estimar los controles establecidos para 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.

Responsabilidades del Líder de Seguridad de la Información de la ANCP-CCE

El líder de Seguridad de la información de la ANCP-CCE deberá cumplir con las siguientes responsabilidades:

- Evaluar, identificar y estimar la brecha entre el Modelo de Seguridad y Privacidad de la información y la situación real de la entidad.

- Proyectar y actualizar los documentos técnicos de Seguridad de la información ANCP-CCE (Políticas, Manuales, lineamientos).

- Promover y mantener un ambiente de cultura y sensibilización de la seguridad de la información para los usuarios de los sistemas, archivos, datos e información de la ANCP-CCE.

- Realizar la sensibilización y capacitación en seguridad de la información y seguridad digital a los usuarios de los sistemas, archivos, datos, e información de la ANCP-CCE.

- Conducir revisiones periódicas de seguridad y privacidad de la información en la infraestructura y sistemas de la ANCP-CCE, para verificar el cumplimiento de las Políticas y normas de seguridad y privacidad de la información.

- Establecer, identificar y coordinar la gestión de riesgos de seguridad de la información de acuerdo con la periodicidad definida.

- Coordinar las actividades correspondientes a la gestión de Incidentes Seguridad de la Información y Seguridad Digital.

- Analizar y evaluar la implementación de las mejoras en las plataformas de la entidad frente a la seguridad de la información (hardware, software, canales de comunicación de datos e infraestructura IT).

- Realizar y/o supervisar los análisis de vulnerabilidades en la ANCP-CCE sobre los diferentes servicios tecnológicos cuya finalidad es detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad.

- Realizar pruebas a los planes de contingencia de continuidad del negocio y requerimientos de recuperación en caso de desastre.

- Solicitar la aprobación a las modificaciones de la política, manuales, lineamientos y demás documentos, procesos y procedimientos al Comité Institucional de Gestión y Desempeño de la ANCP-CCE.

Responsabilidades del Líder de Infraestructura de la ANCP-CCE

El líder de infraestructura de la ANCP-CCE deberá trabajar con el apoyo de cada uno de los administradores de los componentes tecnológicos que soportan la operación del sistema para cumplir con las siguientes responsabilidades:

- Implementar controles para garantizar la seguridad física y lógica de la infraestructura que soporta la gestión, almacenamiento y procesamiento de información de la ANCP-CCE.

- Administrar y gestionar el hardware de las comunicaciones de la red LAN, WLAN y WAN según aplique contractualmente dentro de la ANCP-CCE y asegurar su adecuada operación, manteniéndolos tecnológicamente actualizados.

- Monitorear los enlaces de telecomunicaciones de red WAN principal y de respaldo, enlaces de internet y demás servicios de telecomunicaciones, así como el comportamiento de la red LAN, WLAN y WAN.

- Establecer estándares, procedimientos, control de cambios y responsabilidades de administración y seguridad de cada componente tecnológico y físico que soporta la operación de la ANCP-CCE.

- Garantizar el correcto funcionamiento y administración de la infraestructura tecnológica implementada en los centros de datos Locales o de tipo Cloud disponibles para la ANCP-CCE.

- Desarrollar e implementar una estrategia de backup de la información y configuración almacenadas de la infraestructura tecnológica Local o de tipo Cloud disponibles para la ANCP-CCE.

- Garantizar el adecuado funcionamiento de las plataformas y dispositivos de la infraestructura tecnológica de la ANCP-CCE en ambientes Locales o de tipo Cloud.

- Apoyar en el despliegue de nuevas plataformas tecnológicas que se requieran en la ANCP-CCE.

- Establecer los niveles de acceso, limitar y monitorear el acceso a los datos, código fuente, equipos y demás componentes tecnológicos requeridos por el personal técnico para el desarrollo, mantenimiento, administración, operación y soporte de la ANCP-CCE. En caso de que estos niveles de acceso puedan llegar a comprometer la confidencialidad, disponibilidad o integridad de la ANCP-CCE, deberá contar con la aprobación del Administrador del Sistema de información.

- Monitorear y proyectar los requerimientos de ampliación de capacidad operativa del Sistema de información, a fin de garantizar el procesamiento y almacenamiento requerido.

- Elaborar y realizar pruebas a los planes de contingencia de recuperación en caso de desastre, posteriormente entregará al Líder de Seguridad de la Información el correspondiente informe de las pruebas con evidencias.

- Proporcionar un nivel adecuado de protección a documentos, datos y aplicaciones críticas de conformidad con los estándares y procedimientos de seguridad.

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

- Recabar información para determinar las actividades de tratamiento de los datos personales y acompañar el Registro de las bases de datos en el Registro Nacional de Bases de Datos RNBD de acuerdo con la matriz de activos de información que administra el responsable de seguridad.

- 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

seguridad y privacidad necesarias para la protección adecuada de los 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.

- Si sr 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. POLÍTICAS DE CUMPLIMIENTO ESPECÍFICO

El cumplimiento específico de las Políticas de Seguridad y Privacidad de la Información, recae directamente sobre los funcionarios, contratistas y/o terceros que ejecuten actividades para o en función del objeto social de la ANCP-CCE de forma directa o indirecta, ya que independiente a las tareas realizadas, se presume que en todo momento definido dentro de la ejecución existe exposición a información o sistemas de información de la Entidad debido a sus funciones y a partir de ello se acatarán las Políticas así:

a) Política de Seguridad de los Recursos Humanos.

La ANCP-CCE mantendrá los mecanismos necesarios para asegurar que sus funcionarios y contratistas cumplan con las responsabilidades establecidas en el SGSI de acuerdo con los siguientes lineamientos que se deben aplicar en el momento de la contratación, durante la relación contractual y al finalizar el contrato:

- Incorporar en los procesos de selección de personal los mecanismos para establecer la idoneidad del candidato, y asegurar que conozca su deber

de confidencialidad y seguridad para el manejo de la información a la cual deba acceder en ejercicio de su función y/o responsabilidad.

- Generar conciencia y apropiación en los funcionarios y contratistas, sobre sus responsabilidades en el marco de cumplimiento a las Política General de Seguridad y Privacidad de la Información, con el fin de mitigar los riesgos frente al inadecuado uso de los recursos tecnológicos de la entidad.

- Será reportado por los usuarios cualquier anomalía, debilidad, mal funcionamiento y/o incidente de seguridad de la información identificado en la prestación de algún servicio de Tecnologías de Información y Comunicaciones (TIC) y será reportado a la Subdirección IDT – mesa de ayuda, llamando a la extensión 123, y/o al correo electrónico seguridad@colombiacompra.gov.co.

- Incluir dentro de los documentos legales vinculantes hacia los empleados y contratistas, los recursos jurídicos, clausulas y obligaciones frente al cumplimiento de las Políticas Generales de Seguridad y Privacidad de la Información.

- Divulgar la Política a través de los supervisores de los contratos a: los proveedores, operadores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, obligaciones, compartan, utilicen, recolecten, procesen, intercambien y/o consulten información de la ANCP-CCE.

- Será emitido informe de cierre por parte de todo funcionario o contratista que termina su relación contractual con la ANCP-CCE y tendrá su correspondiente recepción a satisfacción por su jefe directo o quien sea asignado a esta labor.

- Solicitar autorización al área administrativa cuando se requiera retirar de las instalaciones de la entidad activos informáticos, con el fin de registrar, controlar y hacer seguimiento a los mismos. El usuario que retire el activo será el responsable de la custodia, salvaguarda de la información que allí este almacenada.

- Será responsabilidad de los funcionarios, contratistas y pasantes que tengan activos informáticos a su cargo y asumirán las consecuencias en cualquier caso de pérdida o daño que sufran cuando lo anterior no se

ocasione por el deterioro natural, por su uso normal o por otra causa justificada. Cuando se presente eventos de pérdida o daño de activos se procederá a realizar la reclamación a la compañía de seguros.

- Contar con la autorización expresa del usuario titular de la cuenta para acceder a la información del correo electrónico institucional. En caso de investigación previa orden judicial se accederá a la información con base en los protocolos que defina la autoridad competente. En caso de fallecimiento del usuario el acceso será entregado al jefe inmediato y/o supervisor previa solicitud de este.

- Entregar copia de mensajes electrónicos institucionales almacenados en su buzón de correo cuando el funcionario termine su relación laboral o contractual, y/o sea trasladado de dependencia para que estos puedan ser consultados posteriormente, esta actividad será ejecutada por el jefe de área responsable y/o supervisor.

La Secretaría General de la ANCP-CCE debe velar por:

1. Asegurar que los empleados y contratistas comprenden sus responsabilidades frente a la seguridad de la información de la entidad y la idoneidad de acuerdo con el rol que desempeñan.
2. Verificar los antecedentes de todos los candidatos conforme normatividad vigente.
3. Incluir dentro de los documentos jurídicos vinculantes con empleados y contratistas sus responsabilidades y las de la organización en cuanto a seguridad de la información
4. Exigir a todos los empleados y contratistas la aplicación de la Política de Seguridad y Privacidad de la información de acuerdo con los procedimientos establecidos por la organización.
5. Todos los empleados de la organización y los contratistas deberán recibir educación, formación y sensibilización sobre la importancia de la Seguridad y Privacidad de la Información.
6. Incluir obligaciones frente a la responsabilidad y los deberes de Seguridad de la información después de la terminación y/o cambio de contrato.

La Subdirección IDT elaborará un programa sensibilización, capacitación y comunicación en Seguridad y Privacidad de la Información que busque el crecimiento continuo de la conciencia individual y colectiva para la protección de la información en la entidad.

Se debe contar con una definición clara de los roles, así como del nivel de

privilegios correspondientes para el acceso al sistema de contratación pública y los componentes tecnológicos que soportan su operación con el fin de reducir y evitar el uso no autorizado o modificación de la información.

a) Incumplimiento de la Presente Política:

La ANCP-CCE deberá velar por el cumplimiento de las responsabilidades y deberes frente a la Seguridad de la Información, por lo tanto, las siguientes son algunas las actuaciones que pueden causar un incumplimiento de la presente Política:

1. No firmar los acuerdos de Confidencialidad o incumplir dicho acuerdo.
2. Incumplir los lineamientos del presente documento.
3. No reportar oportunamente los Incidentes de Seguridad y/o violaciones a la política de seguridad y privacidad de la información cuando se tenga conocimiento de ello.
4. No cumplir con los controles establecidos por la entidad para la protección de los Activos de Información.
5. Ingresar a sitios restringidos o áreas sensibles sin previa autorización o acompañamiento de personal autorizado.
6. No mantener la Confidencialidad en sus credenciales de acceso a los Sistemas de Información de Colombia Compra Eficiente.
7. Hacer uso de la red interna para obtener, mantener o difundir material relacionado con pornografía, hacking o cualquier otro contenido que vaya en contra del Código de Ética de Colombia Compra Eficiente.
8. Recibir o enviar Información Confidencial de la entidad a través de correos electrónicos personales, diferente al asignado por la ANCP-CCE.
9. Permitir el acceso a la red interna a dispositivos no autorizados.
10. Distribuir o enviar software malicioso utilizando la plataforma tecnológica de la ANCP-CCE.
11. Retirar de las instalaciones de la entidad Información Confidencial sin previa autorización.
12. Instalar software no autorizado en los equipos de trabajo.
13. No cumplir con lo estipulado en Política de Tratamiento de Datos Personales definida por la entidad.

b) Política de Gestión de Activos.

La Secretaría General de la ANCP-CCE, con el acompañamiento permanente de la Subdirección IDT, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información con el objetivo de garantizar su protección.

Dichos lineamientos se impartirán teniendo en cuenta lo siguiente:

- La ANCP-CCE debe llevar un inventario de los activos tecnológicos que manejan.
- La Subdirección de IDT deberá mantener un inventario actualizado de hardware y software informático instalado dentro de la entidad.
- El grupo interno de Infraestructura y Seguridad de SIDT deberá mantener un inventario de los servidores, y equipos de comunicación activos existentes dentro de las instalaciones de la organización o fuera de ella.
- Todos los equipos de cómputo, impresoras, equipos activos y servidores deberán estar etiquetados para su identificación, control e inventario.
- El grupo interno de Infraestructura y Seguridad de SIDT deberá controlar periódicamente y actualizar el inventario de sus respectivos equipos (movilización y/o nueva adquisición).
- La Secretaria General en conjunto con la Subdirección IDT deberán establecer procedimientos para la movilización, adquisición y baja (de manera técnica) de los equipos de la entidad.
- El área de gestión documental de la ANCP-CCE deberá establecer una metodología para la clasificación y rotulado de la información de la ANCP-CCE, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país.
- La ANCP-CCE deberá analizar la autorización del acceso a la red interna por parte de los dispositivos personales de sus funcionarios y contratistas (teléfonos inteligentes, tabletas, portátiles, entre otros). El personal autorizado deberá cumplir los requisitos que defina la ANCP-CCE para incorporar dichos dispositivos a la red interna.
- La gestión y disposición de activos físicos de la ANCP-CCE debe realizarse

con base en un procedimiento de gestión de bienes. La Secretaria General será la encargada de autorizar la baja de un bien.

- Para el caso de reúso de activos tecnológicos, la Subdirección de Información y Desarrollo Tecnológico IDT realizará la generación de copias de respaldo de la información, borrado seguro de medios y demás mecanismos de sanitización establecidos por ANCP-CCE.
- Los funcionarios y contratistas de la ANCP-CCE deben actuar con diligencia en la custodia, cuidado y buen uso de los activos físicos y tecnológicos que se les haya asignado.
- Los Activos de Información serán identificados y clasificados siguiendo los criterios de Confidencialidad, Integridad y Disponibilidad definidos en la metodología definida por la ANCP-CCE y los lineamientos para la divulgación de la información pública disponible.
- La ANCP-CCE mantendrá un inventario de los Activos de Información que soportan los procesos del negocio, cada Activo de Información tendrá un propietario que esté en capacidad de clasificarlo y definir el nivel adecuado de protección que requiera, así como deberá detallar la información contenida y las instalaciones de procesamiento de información.
- Todos los funcionarios y contratistas deberán devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
- La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación y/o a modificación no autorizada, conforme el procedimiento para el manejo de activos y de acuerdo con el esquema de clasificación de información adoptado por la organización.
- La ANCP-CCE implementará procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización, para disponer en forma segura de los medios cuando ya no se requieran, los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
- La ANCP-CCE deberá asignar, formalizar y divulgar los propietarios de los Activos de Información y el alcance de sus responsabilidades, el uso de Activos de Información está destinado para los propósitos que la

entidad defina. Los funcionarios, contratistas y terceros que hagan uso de los recursos tecnológicos de la ANCP-CCE e deben preservar la Confidencialidad, Integridad y Disponibilidad de la información siguiendo las reglas de uso que Colombia Compra Eficiente determine.

c) Política de Control de Acceso

Los propietarios de los activos de información de la entidad, teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de tecnologías e infraestructura física (instalaciones y oficinas), con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física en pro de salvaguardar la integridad, disponibilidad y confidencialidad de la información de la ANCP-CCE, de acuerdo con los siguientes lineamientos:

- Todos los funcionarios, contratistas y terceros que accedan a las plataformas tecnológicas de la ANCP-CCE dispondrán de un usuario y una contraseña (credencial) que deben proteger para garantizar su Confidencialidad, está credencial es de uso personal e intransferible.
- Las contraseñas asignadas deben cumplir con las condiciones de complejidad que defina la ANCP-CCE.
- Cada funcionario, contratista y tercero estará sujeto al debido proceso de gestión de usuarios para la creación, modificación, inhabilitación o eliminación de credenciales bajo el procedimiento que defina la ANCP-CCE, siendo responsables de las actuaciones realizadas con dichas credenciales.
- La ANCP-CCE asignará, modificará o revocará los permisos de acceso de los usuarios a las plataformas tecnológicas, siguiendo el proceso de gestión de acceso lógico y teniendo en cuenta las matrices de roles y perfiles definidas para cada plataforma. La entidad mantendrá los mecanismos de control de acceso físico y lógico para asegurar que los Activos de Información estén protegidos de acuerdo con su clasificación y con la valoración de los riesgos asociados.
- La Subdirección de Información y Desarrollo Tecnológico IDT restringirá las cuentas de usuario con acceso privilegiado a las plataformas

tecnológicas, para ser accedidas solo por el personal autorizado y no deberán ser utilizadas para tareas rutinarias o periódicas del sistema o aplicación.

- La Subdirección de Información y Desarrollo Tecnológico IDT establecerá los mecanismos de control para el monitoreo de las acciones ejecutadas utilizando dichas cuentas.
- La Subdirección de Información y Desarrollo Tecnológico se encargará de configurar los equipos de cómputo para el acceso a la red inalámbrica de la ANCP-CCE.
- Los visitantes solamente tendrán acceso a la red de visitantes, y deben cumplir con los mecanismos de seguridad determinados por el Área de Infraestructura de la ANCP-CCE.
- La ANCP-CCE establecerá las situaciones en las que permitirá el acceso remoto a los recursos tecnológicos y a los Activos de Información, así como, los mecanismos de autorización y conexión a la red interna. Es responsabilidad del funcionario, contratista y/o tercero hacer el uso adecuado del recurso o la información otorgada.
- La ANCP-CCE debe autorizar el acceso a la red interna de los dispositivos personales de sus funcionarios y contratistas como teléfonos inteligentes, tabletas o portátiles. El personal autorizado deberá cumplir los requisitos que defina Colombia Compra Eficiente para incorporar dichos dispositivos a la red interna.
- La ANCP-CCE aplicará los principios de Menor Privilegio y Necesidad de Conocer, para definir los roles y controles de acceso a la información de la entidad según el cargo y las responsabilidades de los funcionarios y contratistas de la entidad.
- Notificarán los jefes de área, supervisores o quien corresponda a la Subdirección IDT cualquier novedad generada a nivel de privilegios de usuario para asignar, modificar o retirar los accesos lógicos a las plataformas y los activos de información. Para el caso de desvinculación del funcionario o contratista, los accesos deben ser removidos por los administradores de sistemas de forma inmediata y las cuentas de acceso deben colocarse en estado inactiva.

La ANCP-CCE establece para su Política de Control de Acceso y apoyando los requisitos del Negocio y de Seguridad de la información el cumplimiento a los

siguientes numerales así:

- Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
- Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
- Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
- Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
- Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se debe retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios a nivel interno.
- Los sistemas de gestión de contraseñas deben ser interactivos y deberían asegurar la calidad de las contraseñas.
- Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
- Se debe restringir el acceso a los códigos fuente de los programas.

d) Política de Criptografía.

La ANCP-CCE dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su Confidencialidad, Integridad y Disponibilidad. El cifrado de la información se realizará de forma transversal a toda la organización sobre los dispositivos, sistemas de información y aplicaciones utilizadas en el día a día para llevar a cabo las actividades propias del Core de Negocio de la ANCP-CCE.

La ANCP-CCE utilizará sistemas y técnicas criptográficas, aplicando controles criptográficos para garantizar la seguridad requerida en los recursos tecnológicos y sistemas de información utilizados por funcionarios, contratistas, proveedores y demás partes interesadas, de igual forma se tendrá una gestión integral sobre

las llaves criptográficas para cuando sea requerido su uso, y es aplicable para plataforma suministrada por la entidad para el desarrollo de las funciones establecidas a nivel contractual, en los siguientes casos:

- La ANCP-CCE implementará herramientas criptográficas debidamente licenciadas que garanticen el aseguramiento de medios (Físicos - Lógicos) a través de algoritmos fuertes de cifrado con la generación de llaves de seguridad requeridas para los procesos de consulta e intercambio.
- La ANCP-CCE aplicará procedimientos de cifrado para la transmisión de la información confidencial fuera de las redes seguras de Colombia Compra Eficiente.
- La ANCP-CCE realizará el resguardo de la información, cuando así lo recomiende la evaluación de riesgos realizada por el propietario de la información y el oficial de Seguridad de la información.
- Las solicitudes de accesos, actualizaciones al sistema o llaves de cifrado se debe efectuar de manera formal a la Subdirección de información y Desarrollo Tecnológico por intermedio del área de seguridad informática.
- Debe existir personas autorizadas responsables de llevar a cabo las solicitudes, tramite y gestión de solicitudes, estas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves criptográficas, así como de la información a la cual se le haya aplicado algún proceso de cifrado.
- El tratamiento de la información que ha sido cifrada o descifrada se debe tratar conforme a su nivel de clasificación y la eliminación deberá realizarse a través de borrado seguro por medio de las herramientas que garanticen el procedimiento y se debe guardar la evidencia del proceso.
- Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.
- Para la administración, gestión y eliminación de llaves criptográficas deberán ser tramitadas por las personas encargadas.
- Las llaves criptográficas deben ser deshabilitadas cuando estas presenten riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con la ANCP-CCE.
- Los funcionarios, contratistas y terceros tendrán la responsabilidad de

reportar, mediante las fallas reales o potenciales de posibles riesgos del sistema de cifrado o firma digital de datos.

- Examinar si los requerimientos de seguridad han sido detallados y aplicadas las medidas de criptografía donde se requiera.
- Es necesario que este alineado con el control A.10.1.2 gestión de llaves.
- Las llaves deben ser lo suficientemente fuertes para tener un equilibrio entre rendimiento y encriptación de la información intercambiada.

e) Política de Seguridad Física y del Entorno

La ANCP-CCE , a través del Oficial de Seguridad de la Información o quien haga sus veces, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como, aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones) con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información de la entidad, de acuerdo a los siguientes lineamientos:

- Todos los servidores públicos, contratistas y visitantes que se encuentren en las instalaciones físicas de la ANCP-CCE deben estar debidamente identificados con su carné, documento y/o distintivo que acredite su tipo de vinculación; en casó de carné debe portarse en un lugar visible.
- Los visitantes en las instalaciones de la ANCP-CCE siempre deben permanecer acompañados por un servidor público o contratista de la entidad debidamente identificado.
- La ANCP-CCE debe asegurar todas sus áreas físicas acorde con el valor de la información que allí sea procesada, almacenada y trasmitida. Los sitios restringidos como cuartos técnicos y/o cualquier otro lugar donde se procese información deberán tener controles de acceso.
- El acceso de personal no autorizado a los cuartos técnicos debe ser aprobado por parte de líder de infraestructura y/o el Subdirector de Información y Desarrollo Tecnológico.
- El acceso a las oficinas de la ANCP-CCE será controlado con filtros

debidamente instalados y gestionados, todo individuo ajeno a la organización o visitante debe ser notificado por escrito y enviar relación al personal encargado de la seguridad física para que permita o restrinja los accesos cuando sea requerido.

- Todo funcionario o contratista que desee ingresar un visitante a las instalaciones de la entidad debe cumplir con el procedimiento de ingreso de visitantes aprobado por la ANCP-CCE.
- La ANCP-CCE dispondrá de equipos de suplencia eléctrica tipo UPS y generador de energía de ser necesario para soportar las fluctuaciones eléctricas, de esta forma se dará alimentación de energía continua a los equipos críticos (Servidores, Comunicaciones, Seguridad etc.), estaciones de trabajo y otros elementos que lo requieran.
- Todos los funcionarios y contratistas de la ANCP-CCE son responsables de bloquear la sesión de su equipo de cómputo en el momento de dejarlo desatendido.
- Todo funcionario garantizará la Confidencialidad, Integridad y Disponibilidad de información impresa, digital o en cualquier medio cuando su puesto de trabajo se encuentre desatendido.
- Los equipos de cómputo tendrán configurado un fondo de pantalla y un protector de pantalla que defina la entidad. Este último, se debe activar después de 3 minutos de inactividad y se desbloqueará mediante el uso de las credenciales del usuario.

f) Política de Seguridad de las Operaciones.

La Subdirección IDT de la ANCP-CCE será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación y velará por la eficiencia de los controles asociados a los recursos tecnológicos de la entidad protegiendo la confidencialidad, integridad y disponibilidad de la información, de acuerdo con los siguientes lineamientos:

- Implementará un comité de control de cambios, para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados.
- Implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba, así como, proveerá la capacidad de procesamiento

requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad.

- Desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de garantizar la disponibilidad de los servicios de TI en el marco de la operación de la ANCP-CCE.
- Realizará respaldo y/o depuración de información almacenada posterior al proceso de finalización de la relación laboral o contractual de un funcionario, y/o sea trasladado de dependencia, el requerimiento de actividad estará a cargo del jefe de área responsable y/o supervisor quien informará a la Oficina de Tecnologías y Sistemas de Información, para poder disponer de los recursos tecnológicos asignados.
- Deberá realizar y mantener copias de seguridad de la información definida para cada proceso de la entidad en medio digital, la Subdirección IDT efectuará las copias respectivas, de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.
- Tendrá a cargo el diseño de un procedimiento bajo la supervisión de la dirección de la Subdirección IDT, con apoyo de los líderes de proceso el cual deberá estar alineado con la gestión documental de la ANCP-CCE, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información. Todo lo anterior asociado a la Política de administración de información y los procedimientos de backup.
- En el evento que alguna dependencia opere una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la ANCP-CCE, se deberá cumplir con lo establecido en la presente Política y los procedimientos dispuestos por el Oficial de Seguridad y de la Información o quien haga sus veces, para tal fin.
- La Subdirección IDT y el área de infraestructura es el área encargada de definir y mantener los procedimientos de respaldo y las herramientas tecnológicas necesarias. Las copias de respaldo de los recursos críticos serán almacenadas en lugares seguros de acuerdo con su clasificación y contarán con las medidas de protección adecuadas. Se realizan copias de

respaldo de la información, del software e imágenes de los sistemas, y se ejecutaran pruebas de funcionalidad de dichas copias de acuerdo con una Política de Respaldo aprobada por la entidad.

- La Subdirección de Información y Desarrollo Tecnológico establecerá las medidas de protección contra código malicioso que afecten el desempeño de los recursos tecnológicos, como herramientas de antivirus, antispyware y demás aplicaciones que considere necesarias.
- Los funcionarios y contratistas no deben desinstalar o desactivar el software o las herramientas de seguridad dispuestas por la entidad, ni está permitido generar, compilar o intentar distribuir cualquier código de programación diseñado para afectar los equipos de cómputo o la infraestructura tecnológica de la entidad.

La Subdirección de Información y Desarrollo Tecnológico es el área responsable de:

1. La revisión y ejecución de las pruebas técnicas sobre los componentes de la infraestructura tecnológica de la ANCP-CCE.
2. Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
3. Asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
4. Separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
5. Generar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
6. Registrar las actividades del administrador y del operador del sistema, y los registros se deben proteger y revisar con regularidad.
7. Sincronizar con una única fuente de referencia de tiempo los relojes de todos los sistemas de procesamiento de información
8. Implementar procedimientos para controlar la instalación de software en sistemas operativos.
9. Establecer e implementar las reglas para la instalación de software por

parte de los usuarios.

10. Implementar la Política de administración de la información.
11. Alinearse conforme la Política de Retención Documental definida en la entidad.
12. Implementar la Política de Transferencia de Información manejada por la entidad en los repositorios autorizados (SharePoint, OneDrive, entre otros.)
13. Implementar la Política seguridad en la nube dando cumplimiento en lo relativo al almacenamiento en la nube.

g) Política de Seguridad de las Comunicaciones.

La Subdirección de IDT establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la ANCP-CCE de acuerdo con los siguientes lineamientos:

- En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio web (web services) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con controles criptográficos y será coordinado por la Subdirección IDT con los mecanismos establecidos para tal fin.
- La Subdirección de IDT debe identificar y gestionar los requerimientos y mecanismos de seguridad para todos los servicios de red que soportan los procesos de la entidad. Adicionalmente, asegurará los componentes de la infraestructura tecnológica, de red y los controladores de dominio de la ANCP-CCE, así mismo, velará por el cumplimiento de los controles de seguridad que establezca para la infraestructura que se encuentra soportada por terceros como los centros de datos alternos, los ambientes tecnológicos en nube y sin limitarse a estos.
  - La ANCP-CCE debe segmentar la red teniendo en cuenta la información, los usuarios y las plataformas tecnológicas. La Subdirección de Información y Desarrollo Tecnológico establecerá e implementará los controles de acceso y tráfico a las redes y subredes con el fin de mejorar su rendimiento y seguridad.

- La ANCP-CCE establecerá los mecanismos y controles para evitar y proteger el acceso no autorizado a la información Confidencial durante su transmisión.
- Cada uno de los funcionarios y contratistas de la ANCP-CCE deberá acatar las políticas establecidas por ANCP-CCE para evitar revelar o transmitir Información Confidencial.

h) Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas.

La Subdirección IDT velará porque el desarrollo y externo de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información de la ANCP-CCE, para lo cual establecerá una metodología que detalle los requerimientos de seguridad interno para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información, de acuerdo con los siguientes lineamientos:

- En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Subdirección IDT es la única dependencia de la entidad con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para la ANCP-CCE, así como, de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la entidad.
- En consecuencia, cualquier software que opere en la ANCP-CCE deberá contar con la autorización de la Subdirección de IDT y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.
- En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional de la ANCP-CCE, deberá cumplir con lo establecido en la presente Política.
- Todo software desarrollado o adquirido por la ANCP-CCE deberá contar

con las respectivas pruebas de seguridad antes de pasar a ambientes productivos dentro de la entidad y se deberá garantizar que el software o sistema de información es seguro para la entidad y para la información que va a procesar.

i) Política de Seguridad para Relación con Proveedores.

La ANCP-CCE a través de la Secretaría General, establecerá, en el Manual de contratación, las disposiciones necesarias para asegurar que la información que se genere custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión del contrato, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los contratistas. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores.

- Todo acuerdo con un proveedor debe estar documentado por medio de un contrato que refleje el objeto contractual por el que fue contratado.
- Se deben establecer acuerdos de confidencialidad con todos aquellos terceros que tengan acceso a información de la ANCP-CCE, independientemente que el proveedor desarrolle su objeto contractual con la subdirección de IDT o con otra área.
- Se deben establecer los riesgos asociados a la cadena de suministro que los proveedores puedan manejar para prestar el servicio contratado por ANCP-CCE.
- La ANCP-CCE deberá realizar auditorías periódicas a sus proveedores revisando que los servicios contratados sean los entregados por el proveedor y que se cumplen las políticas de seguridad de la información.
- Todo cambio de proveedor que procese, almacene, transforme información de ANCP-CCE deberán pasar por un comité de cambios para avalar el cambio de proveedor.

j) Política Gestión de Incidentes de Seguridad de la Información

Se deberá desarrollar y difundir entre todos los usuarios de la ANCP-CCE un mecanismo claro y efectivo para reportar incidentes a la seguridad de la información y continuidad de negocio.

Los incidentes de seguridad de la información deben registrarse de manera exacta y reportarse al grupo interno de Infraestructura y Seguridad de SIDT de forma inmediata y sin dilación.

El líder de seguridad de la información de la agencia o quién haga sus veces, debe recopilar, clasificar, analizar y registrar el reporte de incidentes de seguridad de la información en la entidad, los riesgos, así como, debe tomar las acciones correctivas, para mitigar los riesgos que surjan. En caso de que se afecten datos personales con el incidente, el líder de seguridad de la información tendrá la responsabilidad de notificar al responsable de datos personales de la entidad para que se tomen las acciones concretas en el manejo de incidentes de seguridad que asocien tratamiento de información personal según corresponda.

A los usuarios, internos y externos, involucrados en el incidente, se le respetará el debido proceso apropiado a cada nivel de incidente. Los incidentes que involucren acciones legales o disciplinarias serán remitidos a la instancia que corresponda.

- El reporte de incidentes deberá ser realizado por cualquier miembro de la ANCP-CCE, entre los que se encuentran los funcionarios, terceros, contratistas y todo aquel que identifique una práctica insegura que pueda poner en riesgo la confidencialidad, integridad y disponibilidad de la información.
- El responsable de seguridad de la información o quien haga sus veces deberá dar capacitación al personal de la ANCP-CCE en materia de incidentes de seguridad de la información
- Si el incidente de seguridad de la información no es controlado, el responsable de seguridad de la información deberá convocar al personal necesario y responsable para la activación del BCP de la entidad y del área correspondiente.
- Si durante la investigación del incidente la entidad requiere un análisis forense la ANCP-CCE deberá realizar la respectiva contratación y

documentar los resultados de la investigación.

k) Política de Continuidad

La ANCP-CCE debe contar con un Plan de Continuidad del Negocio para todos sus activos críticos de información priorizado de acuerdo con los resultados del análisis de impacto del negocio (Por sus siglas en inglés - BIA), así como, para todos sus procesos y plataformas asociadas, que le permita preservar la información en caso de una interrupción no deseada o un desastre, de acuerdo con los siguientes lineamientos:

- El Plan de Continuidad del Negocio debe mantener los niveles de Seguridad de la Información establecidos y garantizar la recuperación de los procesos en caso de interrupción de los servicios críticos que lo soportan.
- La ANCP-CCE debe identificar sus operaciones críticas y realizar el diseño de la continuidad de negocio para esas operaciones.
- La entidad debe contar con el personal idóneo para para gestionar el plan de continuidad de la entidad y activarlo en el momento que la ANCP-CCE así lo necesite.
- El plan de Continuidad de Negocio debe estar documentado y divulgado a todo el personal de la entidad.
- El Plan de Continuidad de Negocio debe incluir un plan de recuperación ante desastres (Por sus siglas en inglés - DRP) que permita a la entidad recuperar y proteger la infraestructura tecnológica en caso de presentarse un desastre, así como cualquier estrategia orientada a la continuidad de la prestación del servicio de la ANCP-CCE.
- El plan de Continuidad deberá ser probado con periodicidad por la entidad y deberán realizarse mejoras cada vez que la ANCP-CCE lo requiera basado en los cambios de la entidad.

l) Política de Tratamiento y Protección de Datos Personales.

La ANCP-CCE, cuenta con una Política de Tratamiento y Protección de Datos Personales que se encarga de desarrollar los criterios y lineamientos para el Tratamiento y protección de los Datos Personales en la entidad, así como

informando a los diferentes grupos de interés y a los Titulares de la información, los lineamientos y los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales que se hayan recogido, recibido o que sean tratados a través de los procedimientos, plataformas y en las bases de datos o archivos de propiedad de la Entidad, en cumplimiento de la Ley 1581 de 2012, el capítulo III del Decreto 1377 de 2013 y las demás leyes vigentes y aplicables en la materia. La Política de Tratamiento y Protección de Datos Personales de la ANCP-CCE, se encuentra disponible para consulta en la página web de la entidad.

La ANCP-CCE, deberá disponer de un asesor, funcionario y/o contratista que se encargue del cumplimiento de la Política de Tratamiento de Datos Personales y que implemente los lineamientos de cumplimiento, controles y las medidas administrativas necesarias para la protección de la información personal de acuerdo con lo establecido en las regulaciones vigentes y aplicables.

Así mismo, de forma general de forma interna se deberá cumplir por todos los funcionarios, contratistas, y colaboradores de la entidad con la Política de Tratamiento de datos personales y con todos los lineamientos internos impartidos para el tratamiento adecuado de datos personales, entre los que se encuentran sin limitarse los siguientes:

- Todos los colaboradores, proveedores, funcionarios y/o contratistas de la ANCP-CCE tienen deber y responsabilidad frente a la protección adecuada de la confidencialidad e integridad de la información personal a la que tengan acceso debido a sus funciones, atendiendo al deber de debida diligencia en el uso y tratamiento de la información personal.
- La Secretaría General y el grupo de asuntos jurídicos de la entidad, deberán incluir formatos, acuerdos de confidencialidad y/o cláusulas de protección de datos personales en los documentos establecidos con los funcionarios y contratistas de la entidad.
- El acceso y consulta interno a los datos contenidos en los sistemas de información, herramientas y plataformas de compra pública que administra técnicamente la ANCP-CCE, debe ser clasificado por el área de seguridad de la información e infraestructura por medio de la identificación de roles, perfiles de usuario y permisos, de tal manera que

se tenga acceso únicamente a los datos requeridos para el cumplimiento de las funciones asignadas a cada usuario o rol.

- En el desarrollo de las actividades internas de la entidad desde cada grupo de trabajo, tales como: Talento Humano, capacitación y sensibilización, uso y apropiación, relacionamiento ciudadano, salud y seguridad en el trabajo, contratación, entre otras, en las que se recolecte información personal de contratistas funcionarios, proveedores o ciudadanía en general, se deberá incluir las referencias a la consulta y cumplimiento de la Política de Tratamiento de datos personales de la ANCP-CCE y las autorizaciones de recolección de datos personales.
- La ANCP-CCE, desde la Subdirección de Información y Desarrollo Tecnológico será responsable de la custodia segura y tecnológica de la información personal cumpliendo con las medidas técnicas de seguridad establecidas en el presente documento en cada uno de sus componentes y políticas, será el líder de seguridad el encargado de vigilar el cumplimiento de los controles.
- Se deberán establecer lineamientos adicionales por medio de otros documentos relacionados al adecuado tratamiento de datos personales para el cumplimiento interno y legal en la entidad.

m) Política de Seguridad de la Información en la Gestión de Proyectos.

El Grupo de Planeación de TI de la Subdirección IDT deberá incluir los requerimientos y consideraciones en materia de Seguridad y Privacidad de la Información de los servicios en la metodología de gestión de proyectos de la entidad, garantizando que se implementen en las fases iniciales de los proyectos.

Secretaria General deberá velar que en todos los estudios previos de los proyectos o contratos a celebrar de la ANCP-CCE, se incluyan los requerimientos y consideraciones referentes a Seguridad y Privacidad de la Información, de los servicios que se están contratando.

n) Política de Seguridad Digital.

Todos los servidores públicos o contratistas que hagan uso de los recursos

tecnológicos de la ANCP-CCE tienen la responsabilidad de cumplir cabalmente las Políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por ende, el cumplimiento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

Del Uso del Correo Electrónico.

El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas de la Agencia Nacional de Contratación Pública – Colombia Compra, cuyo uso se facilitará en los siguientes términos:

- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Subdirección de Información y Desarrollo Tecnológico, que cuenta con el dominio @colombiacompra.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
- En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
- La ANCP-CCE implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada de la entidad, de conformidad con la Ley 1712 de 2014.
- Se prohíbe el envío de correos masivos (más de 30 destinatarios) internos o externos, con excepción de los enviados por el área de comunicaciones o las personas autorizadas por la Dirección. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
- Todo mensaje de correo electrónico enviado por la ANCP-CCE plataformas externas deberá hacerse con la cuenta de la entidad y

utilizando el dominio @colombiacompra.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.

- Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a la mesa de ayuda la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.
- Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a La Subdirección de Información y Desarrollo Tecnológico a través de la Mesa de ayuda como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.
- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada de la ANCP-CCE a otras entidades o ciudadanos sin la debida autorización por parte de la Dirección.
- El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.
- El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Subdirección de Información y Desarrollo Tecnológico con el apoyo de la Oficina de Comunicaciones y avalada por la Oficina Jurídica, dicha sentencia debe reflejarse en todos los buzones con dominio @colombiacompra.gov.co.
- Está expresamente prohibido distribuir, copiar o reenviar información de

la ANCP-CCE a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato con la ANCP-CCE, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de secretaria general, por orden judicial, por solicitud de la Oficina de Control Interno o de Control Disciplinario como parte de un proceso de investigación.
- La ANCP-CCE se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del ordenador del gasto, supervisor del contrato, jefe inmediato, Control Disciplinario o de Gestión del Talento Humano.
- Las cuentas de correo electrónico de los funcionarios y contratistas de la ANCP-CCE son personales y de uso exclusivo para el desarrollo de sus funciones. Por lo tanto, la información gestionada a través de este medio es propiedad de la entidad y cada usuario como responsable de su buzón debe cumplir con las condiciones de seguridad definidas.
- Los funcionarios y contratistas no deben utilizar el correo electrónico para el envío de cadenas de correo, mensajes con contenido religioso, político, racista, pornográfico o cualquier tipo de mensaje que atente contra la integridad de las personas, las leyes y la moral. Adicionalmente, el correo electrónico no debe ser utilizado para actividades que comprometan el buen nombre, los Activos de Información o los recursos de la ANCP-CCE.

Del uso de Internet:

La Subdirección IDT, establecerá Políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

- Los servicios a los que un determinado usuario pueda acceder en internet

dependerán del rol o funciones que desempeña en la ANCP-CCE y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.

- Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
- Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por las Políticas de navegación de la ANCP-CCE.
- Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
- Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.
- La ANCP-CCE se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

Del uso de los recursos tecnológicos:

Los recursos tecnológicos de la ANCP-CCE son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del funcionario o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas.
- Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Subdirección de Información y Desarrollo Tecnológico.
- En caso de que el servidor público o contratista deba hacer uso de equipos ajenos a la ANCP-CCE, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado,

actualizado y solo podrá conectarse a la red de la ANCP-CCE una vez esté avalado por la Subdirección de Información y Desarrollo Tecnológico.

- Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- Los funcionarios y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Subdirección de Información y Desarrollo Tecnológico para gestionar la información digital de la ANCP-CCE.
- No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Subdirección de Información y Desarrollo Tecnológico.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Secretaria General, con el fin de llevar el control individual de inventarios.

o) Política de Nube.

Los siguientes ítems presentan las principales actividades que se deben tener en cuenta para la administración de la infraestructura desplegada en nube publica, garantizando una infraestructura de TI flexible y segura, con calidad en los servicios y sistemas tecnológicos de la ANCP-CCE. Por lo tanto, la entidad debe garantizar los siguientes procesos para un buen funcionamiento y operatividad del servicio.

Administración de Acceso Consola de Nube

- Los accesos a los sistemas de administración de nube deben estar definidos y configurados por perfilamiento o roles dependiendo las funciones asignadas en su contrato.
- Todos los servidores públicos o contratistas de la Agencia deben tener acceso únicamente a la información necesaria para el desempeño de sus funciones y será autorizado por el jefe inmediato
- Todos los accesos a los servicios o sistemas desplegados en nube deben cumplir con un mecanismo de autenticación segura con un mínimo de usuario y contraseña.
- Las contraseñas deben ser únicas, personales e intransferibles y por ningún motivo deben ser compartidas.
- Crear un mecanismo de auditoria mediante log en la consola de administración, con la finalidad de identificar acciones realizadas por los usuarios.
- Generarán acciones de monitoreo proactivas de manera constante, con el fin de velar por la disponibilidad de los servicios tecnológicos institucionales de la infraestructura administrada.

Administración y Gestión de Servicios

- Desplegar servicios únicamente en las regiones definidas al interior de la ANCP-CCE, partiendo con los niveles de latencia de las redes por cada una de las nubes referente a nuestra ubicación geográfica.
- Crear grupos de recursos y grupos de componentes por cada sistema de información desplegada o aplicación que garantice la identificación de los componentes.
- Asignar una nomenclatura adecuada al servicio a desplegar en los recursos adquiridos en nube que sean de fácil reconocimiento por los administradores.
- La gestión de los servicios o componentes de infraestructura para los sistemas de información o aplicaciones de la ANCP-CCE, solo deben ser mediante IP interna del segmento de red asignado al proyecto.
- El acceso de administración a los servicios o componentes de infraestructura solo son permitidos con el sistema de VPN asignado por

la ANCP-CCE.

- Solo se asignará IP publica a los servidores Frontend o servicios específicos que por su concepto deben ser publicados a internet para el consumo de los usuarios.
- Los servicios desplegados en nube deben tener asociado un dominio asociado a la función con el dominio propio de la ANCP-CCE.
- Se debe generar una única segmentación por arquitectura o sistema de información que garantice la independización de red entre los servicios desplegados en la nube.
- No se permite intercomunicación entre los servicios de diferentes aplicaciones desplegados en la nube.
- La interoperabilidad entre aplicaciones debe asegurar la comunicación y función de la necesidad de intercomunicación entre servicios
- El área de infraestructura debe entregar a las personas responsables del sistema de información o administrador del servicio los accesos a las plataformas para su debía administración.
- La infraestructura deberá estar funcionando de manera óptima y así garantizar la conectividad y funcionalidad del servicio; a su vez, se entregará por parte de los responsables la evidencia de la entrega y capacitación del correcto uso y operación del componente.
- Supervisar los entornos que ejecutan el mismo sistema operativo, proporcionando gestión de suscripciones, implementaciones, parches y contenido
- Los administradores de nubes deben tener el control de todo lo que se ejecuta y los servicios que se tiene implementado, garantizando la integración, disponibilidad y el uso de las implementaciones existentes.
- La gestión y administración de las aplicaciones o servicios deben estar gestionados desde segmento de red identificado por el administrador de plataforma de la ANCP-CCE
- La Gestión de la configuración de los sistemas informáticos, los servidores y el software en un estado deseado y uniforme es responsabilidad del administrador de la plataforma.
- El software instalado debe estar debidamente licenciado y con autorización de uso para los funcionarios de la entidad.
- Licenciamiento externo a la entidad debe ser reportado por los funcionarios o Contratistas, para que sea validado su autenticidad por el

área de infraestructura.
- Mantener actualizada la información de los perfiles de usuario para los diferentes componentes de tecnología.
- Tener política de cambio de contraseña constante a 90 días para garantizar la seguridad de los accesos a los sistemas tecnológicos.

Seguridad y Monitoreo en nube

- Monitoreo frecuente de los componentes de la plataforma tecnológica a nivel de actualizaciones y respetivo análisis de implementación.
- Presentar plan de trabajo de actualizaciones en el comité de cambios de la Subdirección IDT, los cuales después de la aprobación por parte de los miembros deben ser aplicados garantizando la prestación del servicio en horario hábil, siempre se debe contar con un roll-back.
- Implementar políticas de seguridad de acceso por puertos o ACL (Lista de control de Acceso) a los sistemas desde dentro y fuera de la entidad.
- Implementar sistemas de seguridad perimetral a las aplicaciones que garanticen cualquier tipo de amenaza o ataque cibernético.
- Realizar pruebas de vulnerabilidades en todas las máquinas de los sistemas de información tanto nuevas como antiguas que estén almacenadas en las nubes de la ANCP-CCE.
- Se debe incluir dentro de las políticas de retención, respaldo y recuperación las configuraciones y parametrizaciones de los componentes de la plataforma tecnológica de la Entidad.
- Se debe garantizar la generación de copias de respaldo de la información y del software.

p) Política de Backup

La metodología de despliegue para el plan de copias de seguridad en cinta utilizando Veeam Backup y la tecnología de cinta LTO se estructura de la siguiente forma:

- La ANCP-CCE deberá identificar la información a la cual se le debe realizar backup.
- El área de SIDT definirá la estrategia de backup para la entidad con la

cual se deberán realizar los backups a la información.

- Los backup de ANCP-CCE deberán ser revisados por las partes interesadas y deberán estar listos en caso de requerirse durante los procesos de activación del Plan de Continuidad de Negocio.
- El área de SIDT deberá definir el mejor mecanismo para realizar el backup de la entidad, así como deberá ser responsable de asegurar la ejecución de la estrategia de backup definida.
- La SIDT deberá realizar restauraciones periódicas de la información respaldada y se deberá asegurar que el backup corresponde a la información de los procesos.

Identificación de información crítica

El Jefe de Área o responsable de la información de cada procedimiento, será el responsable de identificar y conservar actualizados los activos de información.
El respaldo de la información de los sistemas integrados relacionados con activos compartidos debe ser solicitado por cada uno de los jefes de área que tienen responsabilidad sobre ellos.

Tipos de Backup

- Incremental: Respaldo de los cambios realizados desde el último backup, realizado diariamente.
- Diferencial: Respaldo acumulativo desde el último backup completo, realizado cada tres días.
- Completo: Copia de toda la información crítica, realizada semanalmente.
- Snapshots: Copias rápidas de los estados del sistema, realizadas antes de actualizaciones críticas.

Frecuencia y tipo de respaldo

La ANCP-CCE, con el apoyo de los expertos contratados para la administración de las plataformas, en conjunto con el responsable de los sistemas de información y el subdirector de IDT, debe definir los tipos de copias de seguridad necesarias para cada Sistema de Información de acuerdo con los requisitos específicos de cada uno.

Para cada copia de respaldo, se deberá considerar la frecuencia de la copia, los medios de almacenamiento, el tipo de contenido, el tiempo de almacenamiento y los procedimientos para el borrado seguro de la información. Esto garantizará que los datos estén adecuadamente protegidos y sean recuperables cuando sea necesario.

Adicionalmente, todas las áreas que generen información deberán definir la frecuencia del respaldo correspondiente y notificar esta información a la Oficina de Planeación y Sistemas, para que sea debidamente registrada en la matriz de activos de información. Esta información será fundamental para mantener un control organizado de los respaldos y la seguridad de los datos en la organización.

Es importante recordar que cada usuario debe utilizar su correo electrónico institucional de manera responsable, guardando la información relacionada con sus funciones o actividades laborales en este espacio. Cabe destacar que la información gestionada a través de la cuenta institucional, en el contexto de las funciones propias del cargo o la ejecución de contratos de prestación de servicios, pertenece a la entidad y no al usuario individual. Por tanto, se recomienda no vincular el correo institucional a plataformas ajenas a la agencia ni usarlo para compartir información personal.

La Agencia promueve el uso de OneDrive como plataforma principal de almacenamiento de información, ya que permite tener acceso a los datos de manera remota, asegurando la disponibilidad y protección de estos. Solo se realiza respaldo de la información contenida en el correo electrónico

institucional y en OneDrive. No se realizan copias de seguridad de la información almacenada en los equipos de cómputo locales, por lo que es responsabilidad de cada colaborador gestionar adecuadamente la seguridad de dicha información.

- Datos críticos: Respaldos diarios.
- Sistemas operativos y configuraciones: Respaldos semanales.
- Aplicaciones y sistemas no críticos: Respaldos mensuales.
- Bases de datos: Respaldos incrementales diarios y completos semanales.

PROTECCIÓN A LOS MEDIOS DE RESPALDO

Los medios de respaldo que contienen información crítica deben estar bajo una custodia estricta que asegure la protección adecuada de los datos almacenados. Esto implica garantizar que dichos medios cumplan con todos los requisitos de seguridad y accesibilidad, de manera que estén listos para ser utilizados en cualquier momento que sea necesario, sin comprometer la integridad o confidencialidad de la información.

Adicionalmente, es fundamental que las copias de seguridad sean almacenadas en ubicaciones secundarias o alternativas. Este enfoque mitiga los riesgos derivados de eventos inesperados que puedan ocurrir en los sitios primarios donde se generan las copias de respaldo, como fallos técnicos, desastres naturales o incidentes de seguridad. De esta manera, se asegura que las copias puedan ser recuperadas en caso de contingencias, garantizando la continuidad de las operaciones.

En el contexto de cambios tecnológicos que puedan generar obsolescencia de los medios de respaldo, es esencial tomar acciones preventivas para resguardar la información almacenada en dichos medios. Esto incluye la actualización de los formatos de respaldo o la migración de los datos a nuevos sistemas o plataformas que aseguren la disponibilidad a largo plazo. Cualquier cambio tecnológico que pueda afectar la integridad o accesibilidad de las copias de seguridad debe ser gestionado adecuadamente para evitar la pérdida de datos importantes o la incapacidad de recuperarlos cuando se necesiten.

q) Política para Dispositivos Móviles

Las políticas para el uso de dispositivos móviles en la ANCP-CCE tienen como propósito establecer los lineamientos y medidas de seguridad necesarias para proteger la información gestionada a través de dispositivos móviles, garantizando la confidencialidad, integridad y disponibilidad de los datos conforme a los requisitos establecidos en el MSPI. Estas políticas buscan mitigar riesgos relacionados con el acceso no autorizado, pérdida de datos y el uso

inadecuado de dispositivos móviles dentro de la entidad.

- Todos los dispositivos móviles utilizados en la ANCP-CCE deben implementar mecanismos de autenticación segura, tales como contraseñas robustas, PIN o autenticación biométrica. Además, se debe aplicar el principio de "mínimo privilegio" para asegurar que solo el personal autorizado tenga acceso a la información confidencial.
- Los dispositivos móviles que manejen información sensible de la ANCP-CCE deben contar con mecanismos de cifrado tanto para el almacenamiento de datos como para las comunicaciones. Esto incluye el cifrado de archivos, correos electrónicos y aplicaciones que puedan contener información crítica.
- La ANCP-CCE establecerá un sistema de gestión de dispositivos móviles (MDM) que permita monitorear, administrar y controlar los dispositivos autorizados para acceder a los recursos de la entidad. Esto incluye la capacidad de borrar de manera remota la información en caso de pérdida o robo del dispositivo.
- Los dispositivos móviles proporcionados por la ANCP-CCE deben ser utilizados exclusivamente para fines laborales. El uso personal de los dispositivos debe ser mínimo y no debe comprometer la seguridad de la información. Cualquier uso indebido será sujeto a las sanciones correspondientes.
- Todos los dispositivos móviles deberán mantenerse actualizados con las últimas versiones de software y parches de seguridad. La ANCP-CCE realizará auditorías periódicas para asegurar el cumplimiento de esta política y evitar vulnerabilidades en los dispositivos.
- El acceso a la red interna de la ANCP-CCE desde dispositivos móviles deberá realizarse exclusivamente a través de conexiones seguras, como redes privadas virtuales (VPN), con el fin de proteger la integridad de la información y evitar accesos no autorizados.
- Es obligatorio que todos los dispositivos móviles cuenten con soluciones de protección contra software malicioso (antivirus, antispyware, etc.) actualizadas, para evitar la infección y propagación de amenazas dentro de la infraestructura tecnológica de la ANCP-CCE.
- Cada usuario de la ANCP-CCE que utilice dispositivos móviles será responsable de su uso seguro, el mantenimiento de la confidencialidad

de la información y la implementación de las medidas de seguridad estipuladas. Cualquier incidente de seguridad relacionado con dispositivos móviles deberá ser reportado inmediatamente a la Subdirección de IDT.

- En caso de pérdida, robo o compromiso de un dispositivo móvil, la ANCP-CCE activará un plan de respuesta rápida para mitigar los riesgos. Esto incluye la desactivación remota del dispositivo, la revocación de credenciales y la notificación inmediata a las áreas correspondientes.

r) Política de Escritorio y Pantallas Limpias

Las políticas de Escritorio y Pantallas Limpias de la ANCP-CCE tienen como finalidad establecer un entorno de trabajo ordenado y seguro, minimizando los riesgos de exposición y acceso no autorizado a información confidencial. Estas políticas son esenciales para mantener la confidencialidad, integridad y disponibilidad de la información conforme a los requerimientos del MSPI, y están orientadas a reducir las amenazas que pueden surgir de documentos sensibles o dispositivos de almacenamiento expuestos.

- Todo el personal de la ANCP-CCE debe mantener su área de trabajo organizada, asegurando que documentos físicos, dispositivos de almacenamiento, y materiales sensibles no queden expuestos al finalizar la jornada laboral o cuando el puesto de trabajo quede desatendido. Documentos y materiales sensibles deben guardarse en cajones o archivadores seguros.
- Se deben configurar los equipos para bloquear la pantalla automáticamente tras un período de inactividad. Es responsabilidad del usuario bloquear manualmente la pantalla al dejar su puesto de trabajo, incluso por periodos cortos.
- Los documentos impresos que contienen información sensible deben ser almacenados en archivadores con llave o en ubicaciones seguras cuando no estén en uso. Los documentos en proceso de eliminación deben ser destruidos adecuadamente utilizando trituradoras de papel con un nivel de seguridad adecuado.
- Los usuarios deben etiquetar claramente los documentos físicos que

contengan información confidencial y manejarlos según los procedimientos de la ANCP-CCE. Está prohibido dejar documentos sensibles en áreas comunes o accesibles por terceros no autorizados.

- Dispositivos previamente autorizados como memorias USB, discos duros externos y otros medios de almacenamiento deben guardarse en lugares seguros cuando no estén en uso. Además, deben ser cifrados para evitar la exposición de información en caso de pérdida o robo.
- Es recomendable minimizar la impresión de documentos sensibles. Cuando sea necesario, los documentos deben recogerse inmediatamente de las impresoras y nunca dejarse desatendidos. La eliminación de documentos debe realizarse mediante procesos seguros, como la trituración.
- La ANCP-CCE llevará a cabo sesiones regulares de concienciación y formación sobre la importancia de mantener un entorno de trabajo seguro. Todos los empleados deberán estar familiarizados con las políticas de escritorio y pantallas limpias y comprender cómo aplicarlas en su rutina diaria.
- Se realizarán revisiones periódicas para asegurar el cumplimiento de las políticas de escritorio y pantallas limpias. Las auditorías internas serán programadas para identificar áreas de mejora y asegurar que se mantenga la disciplina en toda la organización.
- Cada empleado de la ANCP-CCE es responsable de la seguridad de la información en su área de trabajo. El incumplimiento de estas políticas podrá dar lugar a sanciones disciplinarias según lo establecido en las normativas internas de la entidad.

s) Política de Teletrabajo

Las políticas de teletrabajo de la ANCP-CCE tienen como propósito establecer las directrices y medidas de seguridad necesarias para garantizar la protección de la información y la continuidad de las operaciones durante el trabajo remoto. Estas políticas se alinean con los principios de confidencialidad, integridad y disponibilidad de la información, conforme a lo definido en el MSPI, y buscan mitigar los riesgos asociados a la ejecución de labores desde ubicaciones externas a la oficina.

- La ANCP-CCE permitirá el teletrabajo a aquellos empleados cuya naturaleza de trabajo lo permita y quienes hayan recibido la autorización correspondiente. Los empleados autorizados deberán cumplir con los requisitos técnicos y de seguridad establecidos por la entidad.
- Durante el teletrabajo, los funcionarios, contratistas y/o terceros deben cumplir estrictamente con las políticas de seguridad de la información de la ANCP-CCE, incluyendo el uso exclusivo de equipos corporativos o debidamente autorizados para el manejo de información confidencial. Todo acceso a sistemas y recursos debe realizarse a través de conexiones seguras, como redes privadas virtuales (VPN) o mediante protocolos con certificados SSL, TLS o HTTPS en sus últimas actualizaciones o liberaciones más recientes.
- Los empleados en teletrabajo deberán garantizar un entorno de trabajo privado y seguro. No se debe permitir el acceso de personas no autorizadas a la información de la ANCP-CCE, y los dispositivos utilizados deben protegerse mediante contraseñas robustas, cifrado de disco y autenticación multifactor.
- Solo los dispositivos corporativos o aquellos aprobados y configurados conforme a las políticas de seguridad de la ANCP-CCE podrán utilizarse para acceder a la red y sistemas internos. El acceso remoto deberá realizarse con las medidas de seguridad previamente establecidas, como VPN y controles de acceso basados en roles.
- Toda información manejada durante el teletrabajo debe ser tratada conforme a las clasificaciones y niveles de seguridad definidos por la ANCP-CCE. Está prohibido almacenar información confidencial en dispositivos personales no autorizados, y cualquier documento físico debe gestionarse siguiendo las políticas de Escritorio y Pantallas Limpias.
- Los empleados deberán garantizar que los dispositivos utilizados estén actualizados y cuenten con soluciones de seguridad activas, como antivirus y cortafuegos. La ANCP-CCE realizará auditorías y verificaciones periódicas para asegurar el cumplimiento de estas medidas.
- Los empleados deben utilizar los canales de comunicación corporativos para todas las actividades laborales y reportar cualquier incidente de

seguridad inmediatamente. Cualquier duda o problema técnico debe ser informado para su pronta resolución por parte de la Subdirección de IDT.

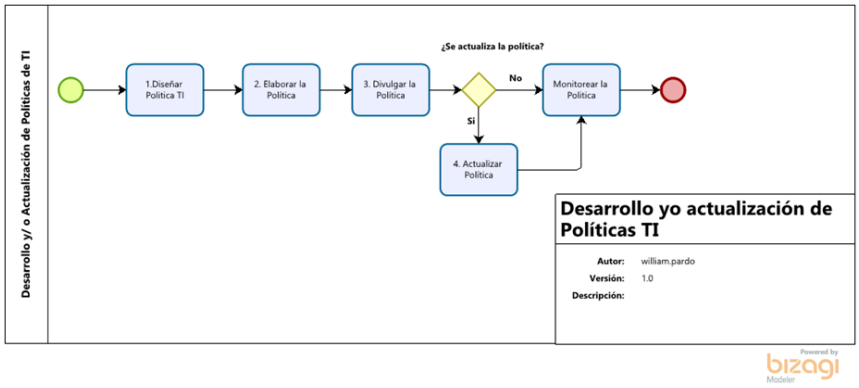
- El teletrabajo debe realizarse de manera que se respete la privacidad de los empleados y se asegure la protección de los datos personales y laborales conforme a la normatividad vigente.
- La ANCP-CCE realizará evaluaciones y auditorías periódicas para verificar la efectividad y el cumplimiento de las políticas de teletrabajo. Cualquier incumplimiento podrá llevar a la suspensión del teletrabajo y a la aplicación de las sanciones correspondientes.
- Los empleados en teletrabajo son responsables de cumplir con todas las políticas establecidas, garantizar la seguridad de la información manejada y mantener un ambiente adecuado para la realización de sus funciones. El incumplimiento de estas políticas estará sujeto a medidas disciplinarias según lo dispuesto por la ANCP-CCE.

9. CICLO DE VIDA DE LAS POLÍTICAS DE TI

Basado en las orientaciones: G.ES.03 Guía del dominio de estrategia: Definición y diseño de una política de TI, se identifican las etapas que hacen parte del ciclo de vida de las políticas de TI.

CICLO DE VIDA DE LAS POLITICAS

Ilustración 1 - CICLO DE VIDA DE LAS POLITICAS



Fuente: Elaboración propia.

10. SEGUIMIENTO Y CUMPLIMIENTO DE LA POLÍTICA

Los controles para seguimiento de una política de seguridad de la información son las actividades que se realizan para evaluar el cumplimiento de la política y detectar cualquier desviación. Estos controles deben ser diseñados para ser efectivos, eficientes y oportunos.

En general, los controles de seguimiento de una política de seguridad de la información se pueden dividir en dos categorías:

- **Controles de gestión**: Estos controles se centran en la gestión de la política y los procesos relacionados. Incluyen actividades como la auditoría, la revisión de la gestión de riesgos, la supervisión del cumplimiento y la formación del personal.
- **Controles técnicos**: Estos controles se centran en la implementación de las medidas de seguridad específicas de la política. Incluyen actividades como la instalación de software de seguridad, la configuración de controles de acceso y la monitorización de los sistemas.
- **Auditorías**: estas evalúan el cumplimiento de la política pueden ser internas o externas, y pueden centrarse en aspectos específicos de la política o en la política en su conjunto. Revisión de la gestión de riesgos: La revisión de la gestión de riesgos es una actividad periódica que se realiza para garantizar que la política sigue siendo adecuada para los riesgos actuales.
- **Supervisión del cumplimiento**: es una actividad continua que garantiza que la organización está cumpliendo con la política. La supervisión del cumplimiento puede incluir actividades como la revisión de registros, la realización de entrevistas y la evaluación de la implementación de medidas de seguridad.
- **Formación del personal**: La formación del personal garantiza que los funcionarios y contratistas conocen la política de seguridad de la información y saben cómo cumplirla. La formación del personal incluye actividades como la formación inicial, la formación continua y la formación en caso de incidentes de seguridad.

11. EXCEPCIONES

La actual Política no tiene excepciones para ninguno de los funcionarios y contratistas de la ANCP-CCE.

12. ACCIONES POR TOMAR DEBIDAS AL NO CUMPLIMIENTO DE LA POLÍTICA

La ANCP-CCE, establecerá los mecanismos necesarios para garantizar el cumplimiento de los requisitos de Ley, las obligaciones contractuales y los lineamientos de Seguridad de la Información establecidos por el SGSI. La entidad debe realizar revisiones periódicas de cumplimiento de la PSPI para garantizar la su aplicación consistente.

El incumplimiento de la PSPI y sus políticas complementarias podrá dar lugar a un proceso disciplinario para los funcionarios y/o un incumplimiento del contrato en el caso de los contratistas. En caso de presentarse un incumplimiento de la Política de Seguridad y Privacidad de la Información, la ANCP-CCE adelantará el proceso disciplinario correspondiente.

En caso de existir incumplimiento de la presente Política y/o los procesos asociados a esta por parte de un contratista o funcionario de la entidad, se comunicará al área de Talento Humano, para que conjuntamente tomen las medidas de sanción respectivas por incumplimiento de acuerdo con las normativas internas, además de las responsabilidades civiles y penales a que hubiere lugar.

El incumplimiento a la PSPI traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

13. ENTRADA EN VIGENCIA.

La Política General de Seguridad y Privacidad de la Información, de la ANCP-CCE, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz.

La presente Política de Seguridad y Privacidad de la Información, rige a partir de su aprobación.

FICHA TÉCNICA DE DOCUMENTO Y CONTROL DE CAMBIOS

1. IDENTIFICACIÓN Y UBICACIÓN	
Título del documento:	Política de Seguridad y Privacidad de la Información
Fecha de aprobación:	03-01-2025
Área / Dependencia de autoría:	Subdirección de Información y Desarrollo Tecnológico
Resumen / Objetivo de contenido:	En el presente documento se establecen las directrices, lineamientos y las medidas organizacionales de seguridad que permitan proteger, asegurar y fortalecer la adecuada gestión de la seguridad y privacidad de la información de la ANCP-CCE.
Código de estandarización:	CCE-GTIIDI-01
Categoría / Tipo de documento:	Política
Aprobación por:	CIGD en sesión del 12/12/2024
Información adicional:	N/A
Serie documental según TRD	POLITICAS
Enlace de ubicación original del documento (especifique donde se aloja o reposa el documento)	POLITICAS

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN				
ACCIÓN	**NOMBRE**	**CARGO/ PERFIL**	**FECHA**	**FIRMA**
Elaboró	Cevallos & Holguín Consultores S.A.S	Contratista IDT	09/08/2024	Original firmado
Revisó	COASIC	Comité Asesor en materia de seguridad de la información	05/12/2024	Acta Comité
Aprobó	CIGD	Comité Institucional de Gestión y Desempeño	12/12/2024	Acta Comité sesión 12-12-2024
Nota: Si la aprobación se realizó mediante acta de alguno de los comités internos considerados en la resolución número 173 de 2020 por favor especificar acta y mes del desarrollo de esta.				

3. CONTROL DE CAMBIOS DEL DOCUMENTO					
VERSION	**AJUSTES**	**FECHA**	**VERSIÓN VIGENTE DEL FORMATO**		**04**
01	Elaboración del documento	23/05/2016	**Elaboró**	Santiago Carvajal Torres	Contratista líder de seguridad
			Revisó	María Margarita Zuleta González	Director(a) General de la Agencia
			Aprobó	Comité Directivo e Institucional	Comité Directivo e Institucional
02	Actualización del documento	22/12/2020	**Elaboró**	Milena Cabrales	Contratista IDT
			Revisó	Rigoberto Rodríguez	Subdirector IDT
			Aprobó	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño
03	Actualización del documento	20/01/2023	**Elaboró**	Diego Andrés Vega Castillo	Contratista IDT
			Revisó	Ana Maria Cárdenas y Walter Triana	Contratista IDT Coordinador de Infraestructura y Seguridad de la Información

			Aprobó	CIGD	Acta CIGD 19/12/2022
04	Actualización general del documento	03/01/2025	**Elaboró**	Cevallos & Holguín Consultores S.A.S	Contratista IDT
			Revisó	COASIC	Comité Asesor en materia de seguridad de la información
			Aprobó	CIGD	Comité Institucional de Gestión y Desemepeño

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