2023

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA
-COLOMBIACOMPRA EFICIENTE-

ENERO 2023

CONTENIDO

INTRODUCCIÓN

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), alineado a la política 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.

I. 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 SGSI de la entidad, con el fin de evitar, prevenir y mitigar los riesgos que comprometan los principios de seguridad de la información.

II. OBJETIVOS ESPECIFICOS

1. 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.

2. Mitigar el impacto de los incidentes de seguridad, y privacidad de la información de forma efectiva, eficaz y eficiente.

3. 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.

4. 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.

5. 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.

6. Definir, operar y mantener el Plan de Continuidad del Negocio para las Plataformas de la ANCP-CCE.

III. ALCANCE Y APLICABILIDAD

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:

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

IV. MARCO LEGAL

Constitución Política de Colombia -Artículo 15.
Ley 594 de 2000 - Por medio de la cual se expide la Ley General de Archivos.
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.
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"
Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 de 2015 _ Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
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.

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.
Decreto 1377 de 2013 -Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1083 de 2015 - Único Reglamentario del Sector Función Pública y las modificaciones introducidas al Decreto Único Reglamentario del Sector de Función Pública a partir de la fecha de su expedición.
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.
Decreto 1078 de 2015 - Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
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.
Conpes 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Conpes 3854 de 2016. Política Nacional de Seguridad Digital.
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.

Guía-Modelo de Privacidad y Seguridad de la Información MSPI- MinTIC.
Guía -Modelo de Gestión de Riesgos de Seguridad Digital -MinTIC
NTC-ISO/ICE 27001 y NTC-ISO/ICE 27002. Para la gestión de la privacidad de la información.
ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.

V. DEFINICIONES Y/O GLOSARIO.

Con el propósito de facilitar la comprensión de la presente Política se deben tener en cuenta las siguientes 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.
Antivirus: Software cuya función es detectar y/o eliminar virus informáticos
Ambiente: conjunto de elementos o componentes tecnológicos o, grupos de sistemas de información, en los cuales reside o fluye información y datos de negocio.

Ataques de denegación de servicio: también llamado ataque DoS es un ataque a una aplicación o una maquina o red informática que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

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.

Cifrado Asimétrico: Método criptográfico que usa un par de llaves relacionadas matemáticamente entre sí para el envío de mensajes. Una de las llaves es pública y es usada para cifrar el mensaje, la otra llave es privada y permite descifrar el mensaje cifrado con la llave pública.

Cifrado Simétrico: Método criptográfico que emplea la misma llave para cifrar y descifrar un mensaje.

Código móvil malicioso: Se trata de virus, troyanos, gusanos o programas "broma", es decir, que simulan ser virus sin serlo

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.

Custodio o usuario de un equipo computacional: Empleado de la Organización que tiene el control físico o tenencia del equipo computacional y es el responsable de vigilar o proteger el activo tecnológico en mención.

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.

Incidente de seguridad: Es un evento o serie de eventos no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
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.
Incidente: Una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI.
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
Logs de Seguridad: Este tipo de Log registra sucesos que tengan relación directa con la disponibilidad, confidencialidad, e integridad de la información.
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.
No Repudio: Es la irrenunciabilidad, es decir, permite probar la participación de las diferentes partes en una comunicación.
Onedrive: Es un servicio para almacenamiento virtual en la nube de la información pública de las áreas de la institución.
Oficial de Seguridad de la Información: en inglés, CISO (chief information security officer: 'oficial principal de seguridad de la información')– es el responsable máximo en planificar, desarrollar, controlar y gestionar las Políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.
Oficial de Protección de Datos Personales: hace referencia a la persona, área, grupo, contratista que asume la función de protección de datos personales en la entidad y que dará trámite a las solicitudes de los titulares de la información, velando por la implementación efectiva de los procedimientos para la gestión de los datos personales.
Política de Tratamiento de Datos Personales: Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

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: es una 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: son un 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.

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

Titulares de la Información personal: Persona natural cuyos datos personales sean objeto de Tratamiento

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.

SharePoint: Sitio para almacenamiento de la información pública para uso interno de la institución

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, [Magerit: 1997].

Virus informático: es un software que tiene por objetivo de 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.

VI. PRINCIPIOS

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:

1. 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.
2. 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.
3. 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.
4. 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.

VII. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

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 su información de las amenazas originadas por parte del personal interno y/o externo que tenga acceso a la información de la entidad.
- La ANCP-CCE protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos implementado 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 que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- 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 que utilizan, supervisan y administran los sistemas de la ANCP-CCE que manejan información que reside en su infraestructura, plataformas y equipos.

Por lo tanto, la entidad debe definir las responsabilidades frente a la Seguridad 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 del(os) 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 del Sistema 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 asesor 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.
- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados en 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.
- Planear estrategias para optimizar el comportamiento de los enlaces de comunicaciones a nivel LAN, WLAN y WAN de la ANCP-CCE para garantizar un funcionamiento estable de la misma.
- 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 el centro de datos On-Premise de la ANCP-CCE.
- Desarrollar e implementar una estrategia de backup de la información y configuración almacenadas de la infraestructura tecnológica de la ANCP-CCE (On-Premise).
- Garantizar el adecuado funcionamiento de las plataformas y dispositivos de la infraestructura tecnológica de la ANCP-CCE (On-Premise).
- 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.

Responsabilidades del asesor o contratista para la Protección de datos personales

- Garantizar el ejercicio de los derechos de los Titulares de la Información personal.
- Tramitar, proyectar y contestar las consultas y reclamos sobre protección de datos personales de los usuarios, titulares y/o áreas internas de la ANCP-CCCE.
- Tramitar los requerimientos ante la autoridad correspondiente y/o contestar los requerimientos de los titulares de la información personal.
- Implementar dentro de la entidad, el cumplimiento de las obligaciones para la protección de los datos personales que sean aplicables (Políticas, autorizaciones, avisos de privacidad, sensibilización y capacitación).
- Coordinar con los líderes de los equipos de seguridad de la información, infraestructura interna y los administradores de los sistemas de compra pública que se cumpla con las medidas de seguridad y privacidad necesarias para la protección de los datos personales.
- Registrar las bases de datos en el Registro Nacional de Bases de Datos ante la autoridad competente.

Responsabilidades de los usuarios de la información de la ANCP-CCE

Los usuarios son todos los funcionarios y/o contratistas de la ANCP-CCE que utilizan la información de los sistemas de información de la Entidad debido a sus funciones y/o actividades, deben tener responsabilidades debido a su interacción con la información de la Entidad.

b) 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:

- 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.

- Será La Subdirección IDT de la ACNP-CCE, quien deberá desplegar esfuerzos para generar conciencia y apropiación de los funcionarios y contratistas, sobre sus responsabilidades en el marco de la Política General de Seguridad y Privacidad de la Información, con el fin de mitigar los riesgos frente al mal uso de los recursos tecnológicos de la entidad y así asegurar la confidencialidad, integridad y disponibilidad de la información.
- En el proceso de selección de personal de nómina y/o de prestación de servicios, la ANCP-CCE debe incorporar 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.
- Todos los usuarios que identifiquen cualquier anomalía, debilidad, mal funcionamiento y/o incidente de seguridad de la información en la prestación de algún servicio de Tecnologías de Información y Comunicaciones (TIC) deberán reportarlo a la Subdirección IDT – mesa de ayuda, llamando a la extensión 123, y/o al correo electrónico seguridad@colombiacompra.gov.co.
- La Secretaria General incluirá en las minutas de los documentos jurídicos vinculantes, cualquiera que sea su naturaleza y/o modalidad, cláusulas y obligaciones, el referente al cumplimiento de la Política General de Seguridad y Privacidad de la Información de la ANCP-CCE.
- La presente Política deberán ser divulgada 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.
- Cuando un usuario termine su relación laboral y/o contractual con la entidad, el jefe de área y/o supervisor deberá informar a los líderes funcionales y técnicos de los sistemas de información de la ANCP-CCE según corresponda y a la Subdirección IDT, para retirar los accesos lógicos a las plataformas y los activos de información. Los accesos deben ser removidos por los administradores de sistemas de forma inmediata y las cuentas de acceso deben colocarse en estado inactiva.
- Cuando un usuario sea trasladado de dependencia o cargo, el jefe de área y/o supervisor deberán informar a los líderes funcionales y técnicos de los sistemas de información según corresponda y a la Subdirección IDT, para retirar los accesos lógicos a los activos de información a los cuales tenía y/o añadir los accesos que se requiera.
- Cuando un usuario termine su relación laboral, contractual y/o sea trasladado de dependencia, el jefe de área responsable y/o supervisor deberán verificar la entrega de la información en los repositorios de red autorizados para garantizar su preservación y conservación.

- Cuando un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia el jefe de área responsable y/o supervisor deberán informar a la Oficina de Tecnologías y Sistemas de Información, para hacer limpieza de la información almacenada en las estaciones de trabajo antes de la asignación del equipo.
- Cuando un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia el jefe de área responsable y/o supervisor deberán verificar que los activos asignados a los funcionarios, contratistas, pasantes o proveedores sean devueltos a la Subdirección Administrativa para el control de inventarios en las condiciones y estado en que le fueron entregados.
- Cuando se requiera retirar de las instalaciones de la entidad activos informáticos, se deberá solicitar autorización al área administrativa, 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.
- Los funcionarios, contratistas y pasantes que tengan activos informáticos a su cargo, son responsables de la 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.

- Para acceder a la información del correo electrónico institucional, se debe contar con la autorización expresa del usuario titular de la cuenta. 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.
- Cuando un usuario termine su relación laboral o contractual, y/o sea trasladado de dependencia el jefe de área responsable y/o supervisor deberán verificar que el usuario entregue copia de los mensajes electrónicos institucionales almacenados en su buzón de correo, para que estos puedan ser consultados posteriormente.

La secretaria 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 acceso y los 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.

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.

c) 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 re-uso 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. En caso de pérdida o daño de un recurso tecnológico el funcionario o contratista debe informar inmediatamente a la Subdirección de Información y Desarrollo Tecnológico.
- La ANCP-CCE se reserva el derecho de monitorear el acceso y uso de los recursos electrónicos asignados a los funcionarios o contratistas de la entidad. La Subdirección de Información y Desarrollo Tecnológico es el área encargada

de hacer las modificaciones o actualizaciones en los elementos y recursos tecnológicos.

d) 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.
- Los funcionarios, contratistas y terceros deben solicitar la creación, modificación, inhabilitación o eliminación de credenciales siguiendo el proceso de gestión de acceso lógico 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 deberá contar con una Política de control de acceso con base en los requisitos del negocio y de Seguridad de la información. Donde se especifica los siguiente:

- 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 propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
- 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.
- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la Política de control de acceso.
- Cuando se requiera, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
- 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.

e) 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 por solicitud de los usuarios o de manera general cuando así lo requiera la entidad.

La ANCP-CCE utilizará sistemas y técnicas criptográficas para:

- La protección de claves de acceso a sistemas, datos y servicios;
- La transmisión de Información Confidencial fuera del ámbito de ANCP-CCE y;
- El resguardo de información, cuando así lo recomiende la evaluación de riesgos realizada por el propietario de la información y el oficial de Seguridad de la Información.

f) 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.
- 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.

- 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.
- En el caso que un funcionario o contratista de la entidad tenga bajo su custodia un documento físico clasificado como Información Confidencial, deberá mantenerlo bajo llave 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.

g) 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.
- Deberá realizar y mantener copias de seguridad de la información 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 ANCP-CCE mantendrá un esquema de copias de seguridad sobre los recursos críticos de cada proceso de negocio, asegurándose de tener la capacidad de restaurar de forma completa y oportuna la información en caso de ser necesario.
- 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.

h) 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 service) 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.
- En el caso de persona jurídica proveedora de servicios para la ANCP-CCE, en la respectiva carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrita por el representante legal de dicha persona.
- 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.
- La ANCP-CCE debe segregar 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 tomar las

medidas necesarias para evitar revelar o transmitir Información Confidencial.

- 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.

i) 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.

j) 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.

k) 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.

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 debe recopilar, clasificar, analizar y registrar el reporte de incidentes de seguridad de la información en la entidad, así como debe tomar las acciones correctivas, para mitigar los riesgos que surjan.

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.

l) Política de continuidad

La ANCP-CCE debe contar con un Plan de Continuidad del Negocio para todos sus activos críticos de información, 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.
- El Plan de Continuidad de Negocio debe incluir un plan de recuperación ante desastres 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.

m) Política de Tratamiento y Protección de Datos Personales.

La ANCP-CCE deberá disponer y contar con un asesor para la protección de datos personales o quien haga sus veces con el fin de ejecutarla implementación de los lineamientos, los controles y las medidas administrativas necesarias para la protección de la información personal de acuerdo con lo establecido en las regulaciones vigentes y aplicables.

Por lo tanto, la ANCP-CCE, en cumplimiento de las disposiciones establecidas en la Ley 1581 del 17 de octubre de 2012, sus decretos reglamentarios y las demás normas que la modifiquen, deroguen o subroguen deberá contar con una Política de Tratamiento y Protección de Datos Personales que deberá estar disponible para su consulta en la página web de la entidad https://colombiacompra.gov.co/transparencia/politicas-y-lineamientos documento que regula la responsabilidad que le asiste a la Entidad en materia de Tratamiento de Datos Personales y el manejo de la información personal de acuerdo con la normatividad vigente y aplicable.

Así mismo, de forma general se deberá seguir de forma interna por todos los funcionarios, contratistas, y colaboradores los siguientes lineamientos de seguridad para el tratamiento de los datos personales:

- Todos los colaboradores, funcionarios y/o contratistas de la ANCP-CCE serán responsables en su deber frente a la protección de la confidencialidad e integridad de la información personal a la que tienen acceso en razón de sus funciones, atendiendo al deber de debida diligencia en el uso y tratamiento de la información personal
- La Secretaría General deberá incluir y/o recolectar el consentimiento y la autorización necesaria para el tratamiento de los datos personales de los funcionarios y contratistas, de acuerdo con los lineamientos del oficial y/o líder para la protección de datos personales.
- El acceso interno a los datos contenidos en los sistemas de información y de compra pública de la ANCP-CCE, debe ser clasifica por roles y/o perfiles de usuario, de tal manera que se tenga el acceso únicamente a los datos requeridos para el cumplimiento de las funciones asignadas al usuario.
- En el desarrollo de las actividades internas de la entidad (Talento Humano, capacitación, salud y seguridad en el trabajo, etc.), en las que se recolecte información personal de contratistas y/o funcionarios, deberá incluirse las referencias a la consulta y cumplimiento de la Política de Tratamiento de datos personales de la ANCP-CCE.
- 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 de seguridad de la información y de la normatividad vigente y aplicable.

n) 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.

o) 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:

a. 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.

b. 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:

c. 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.

d. 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.

VIII. CONTROL DE CUMPLIMIENTO Y SANCIONES

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 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.

IX. ENTRADA EN VIGENCIA.

La Política 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:	20-01-2023
Resumen / Objetivo de contenido:	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.

Area / Dependencia de autoría:	Subdirección de Información y Desarrollo Tecnológico
Código de estandarización:	CCE-IDT-GI-03
Categoría / Tipo de documento:	Plan
Aprobación por:	CIGD
Información adicional:	NA
Serie documental según TRD	
Enlace de ubicación original del documento (especifique donde se aloja o reposa el documento)	https://cceficiente.sharepoint.com/:f:/g/cce/Ev9SH4kNlhVMue4fk4kABAsBCDnXUokkaruY9lWyyv5lRA?e=GcuNkS

2. AUTORES Y RESPONSABLES DE REVISIÓN Y APROBACIÓN

ACCIÓN	NOMBRE	CARGO/ PERFIL	FECHA	FIRMA
Elaboró	Diego Andrés Vega Castillo	Contratista	05/05/2022	
Revisión Jurídica	Ana María Cárdenas	Contratista	16/05/2022	Ana M Cárdenas
Revisó	Walter Triana	Coordinador de Infraestructura y Seguridad de la Información	19/12/2022	
Aprobó	Rigoberto Rodríguez Peralta	Subdirector de IDT		Firmado digitalmente por RIGOBERTO RODRIGUEZ PERALTA Fecha: 2023.01.25 16:19:28 -05'00'

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.

CONTROL DE CAMBIOS DE DOCUMENTO

Versión vigente del documento: 03

VERSIÓN	FECHA	DESCRIPCIÓN DE AJUSTES	ELABORÓ	REVISÓ	APROBÓ
1	23/05/2016	Creación del documento	Santiago Carvajal Torres	María Margarita Zuleta González	Comité Directivo e Institucional de Desarrollo Administrativo de Colombia Compra Eficiente

2	22/12/2020	Actualización del documento	Milena Cabrales Contratista Líder de Seguridad	Rigoberto Rodríguez subdirector de IDT	Comité Institucional de Gestión y Desempeño
3	20/01/2023	Actualización del documento	Diego Andrés Vega Castillo	Ana Maria Cárdenas Walter Triana Rigoberto Rodríguez Peralta	Aprobado Comité de Gestión y Desempeño Institucional- sesión 19 de diciembre de 2022

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.