POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PARTE INTEGRAL DEL MANUAL DEL SGSI DE ARTESANÍAS DE COLOMBIA

ARTESANÍAS DE COLOMBIA

JULIO 2021

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las políticas complementarias alineadas a la política de alto nivel del Sistema de Gestión de Seguridad de la Información SGSI de Artesanías de Colombia, en adelante AdC, en pro de gestionar adecuadamente la integridad, confidencialidad y disponibilidad de los activos de información, en el marco de la NTC/ISO 27001:2013 y su Anexo A.

2. GENERALIDADES

El presente documento de políticas específicas de seguridad de la información, hace parte integral del modelo de seguridad adoptado por AdC y establecido en el Manual del SGSI.[1]

3. APLICACIÓN

Las políticas de seguridad de la información establecidas en este documento, han sido orientadas para los procesos, servidores públicos, contratistas, pasantes, proveedores y terceros, que dependan o interactúen con AdC, en términos de seguridad de la información.

4. ALCANCE

Las políticas de seguridad de la información de AdC presentadas en este documento, aplica a todos los activos de información de la entidad durante su ciclo de vida (creación, distribución, transmisión, almacenamiento y eliminación); están orientadas a proteger

---

[1] Ver Manual del SGSI de AdC

los activos de información en todos los ambientes en los cuales reside y a asegurar que estén sometidos a controles equivalentes para su protección.

5. DEFINICIONES

Acceso lógico: Es un acceso en red a través de la intranet de la entidad o de Internet.

Activo: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Activos de Información: Los activos de información son datos o información propietaria en medios electrónicos, digital, impreso o en otros medios, considerados sensitivos o críticos para los objetivos del proceso.

Almacenamiento: Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, áreas seguras, cajas, PC's, Servidores, CD's, DVD's, USBs, cintas magnéticas, etc.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

Área solicitante: Es la dependencia de AdC que solicita al funcionario competente y/u ordenador del gasto, la contratación de bienes o servicios para satisfacer necesidades o solucionar problemas.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Base de Datos: Conjunto organizado de datos personales, institucionales o corporativos que sea objeto de Tratamiento;

Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo magnético y enviado a través de una red de datos mediante la codificación de llave o clave privada y pública (letras, símbolos o números) del contenido que sólo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Contraseña: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

Contratista: Persona natural o jurídica que se vincula a la Entidad con el objeto de prestar a la misma un bien o un servicio determinado.

Creación: Se refiere a la concepción de documentos o datos, en el momento en el cual se origina el contenido (digital o físico) de un medio de información.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, privilegios de acceso, modificación y borrado

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada

Destrucción: Se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida

Incineración: Destrucción de información exponiéndose a altas temperaturas para quemarla.

Borrado seguro es un método de borrado de archivos basado en software cuya función es sobrescribir los datos con el propósito de destruir completamente todos los datos electrónicos que residen en una unidad de disco duro u otros medios de almacenamiento. El borrado seguro busca la eliminación permanente de los datos, por lo que va más allá de los comandos básicos de eliminación de archivos, que sólo eliminan los punteros a los sectores de disco que contienen los datos, haciendo posible la recuperación de datos con herramientas de software comunes.

Trituración: Esto aplica a la destrucción de papel por medio de máquinas trituradoras.

Dominio: Áreas en las que se desarrolla la norma NTC/ISO 27001:2013.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Etiquetado: Colocar una etiqueta o rótulo para identificar un elemento.

Evento de Seguridad de la Información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Incidente de seguridad de la Información: Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.

Integridad: Propiedad de la información relativa a su exactitud y completitud

Lineamientos: Describe en orden numérico y de acuerdo a su importancia las directrices específicas establecidas para la aplicación de la política.

Medio Removible: Dispositivos de almacenamiento independientes del computador que pueden ser transportados libremente. Los más comunes son: Memorias USB, discos duros extraíbles, DVD y CD.

Política de seguridad de la información: Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.

Programas Utilitarios: Son programas diseñados para realizar una función determinada, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.

Propietario de la información: Es el responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Rol: El papel que desempeña un individuo o un grupo en una actividad determinada.

Seguridad de la Información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

Servidor Público: Persona que desempeña un empleo público. Se trata de un trabajador que cumple funciones en el organismo del estado.

Sistema de procesamiento de información: Es un sistema que transforma los datos en información organizada, significativa y útil.

Teletrabajador: Persona que utiliza las tecnologías de la información y comunicación como medio para realizar su actividad laboral fuera de las instalaciones físicas del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.

Teletrabajo: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las Tecnologías de la Información y la Comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Token de seguridad: (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación y no repudio de los procesos realizados. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales.

Transporte de datos: Son las diferentes formas en la que se transporta la información de un lado a otro y los cuidados que se debe tener en este proceso, según su nivel de clasificación.

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

Usuario: Individuo que utiliza una computadora, un sistema operativo o cualquier sistema informático. Por lo general es una única persona.

VPN: (Virtual Private Network) La tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet, es considerada como una extensión segura de la red local o LAN.

6. NORMAS APLICABLES

Nomograma del SGSI

Ley estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013, por el cual se reglamenta parcialmente la ley 1581 de 2012.

Ley 1712 de 2014, Derecho de Acceso a la Información Pública

Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.

Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información.

Norma Técnica Colombiana NTC-ISO/IEC 9001 Sistema de Gestión de la Calidad.

Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.

7. INTRODUCCIÓN

La adopción de Políticas, y procedimientos en AdC, obedece a una decisión estratégica que cumple con las normas de Seguridad y Privacidad de la Información, éstas deben analizarse, diseñarse e implementarse para satisfacer las necesidades, los objetivos, los requisitos de seguridad, los procesos, el tamaño, la tecnología y la estructura de la entidad.

En la actualidad, AdC identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en el Plan Estratégico de la

Entidad, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada.

Adicional a lo expuesto, en la medida en que los sistemas de información se constituyen en un apoyo de los procesos de AdC, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la información.

Las Políticas de seguridad establecen los objetivos e identifican y definen las responsabilidades para una protección apropiada de los activos de información de la Entidad, por ello con su implementación, se busca reducir el riesgo de que en forma accidental o intencional se divulguen, modifiquen, destruyan o usen en forma indebida

De igual forma, con la adopción de las políticas de seguridad de la información, se busca que AdC fortalezca la administración de la seguridad de sus activos de información, apoyados en controles tecnológicos, administrativos, operativos y físicos en los que intervienen personas, generando que las políticas contemplen los siguientes aspectos:

- Ser Holísticas, es decir, que la seguridad se debe ver como un todo de manera global e integrada.
- Que se adecuen a las necesidades reales y recursos de la entidad.
- Que definan estrategias y criterios generales a cumplir en distintas funciones y actividades que se ejecutan dentro de AdC.
- Que AdC definan las reglas de operación para la protección de la información apoyados en el marco de la normatividad Legal Vigente relacionada con la Seguridad de la Información y la Estrategia de Gobierno Digital.

Por lo anterior, se establece la política general de seguridad de la información y las políticas específicas de seguridad y privacidad de la información, basados en los dominios de la norma ISO 27001:2013, las cuales ayudarán a ofrecer servicios seguros, confiables y oportunos en la Entidad.

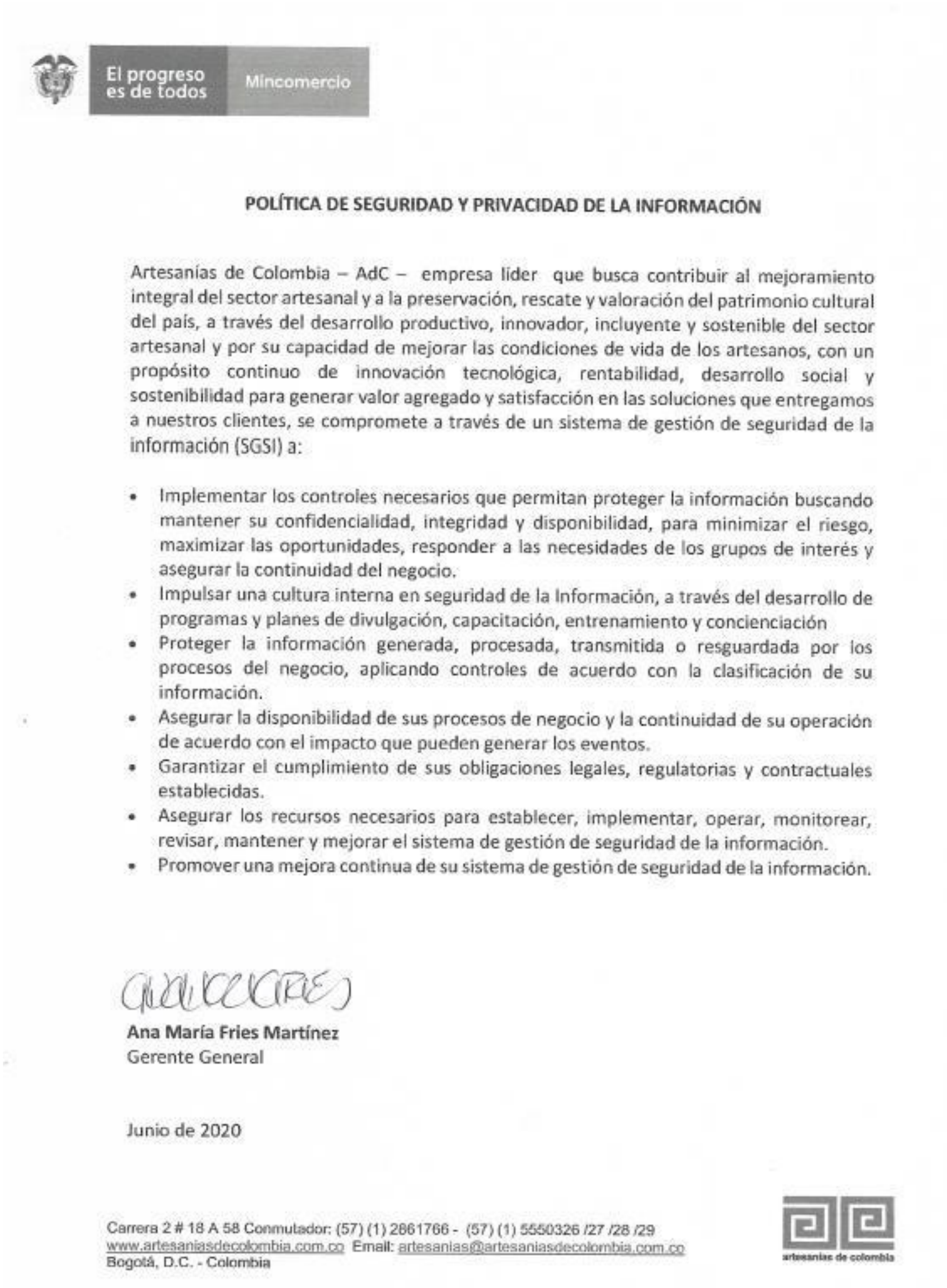
Política general de seguridad de la información: establece la política de alto nivel con respecto a la seguridad de la información de AdC.

Las políticas específicas, se desarrollan teniendo en cuenta los dominios y los controles definidos en el Anexo A de la norma y la declaración de aplicabilidad.

Teniendo en cuenta lo expuesto, AdC, define sus políticas, por medio de las cuales asegura y mantiene la Confidencialidad, Integridad y Disponibilidad de la Información; por tanto cada política es revisada, aprobada, establecida y socializada desde la alta dirección a todos los niveles de la Entidad, incluyendo servidores públicos, contratistas, proveedores, pasantes y terceros, para su estricto cumplimiento.

8. POLÍTICA DE ALTO NIVEL DEL SGSI

Armonizados con el Plan Estratégico Institucional, la Entidad establece como política de alto nivel del SGSI, la siguiente:



El progreso es de todos
Mincomercio

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Artesanías de Colombia – AdC – empresa líder que busca contribuir al mejoramiento integral del sector artesanal y a la preservación, rescate y valoración del patrimonio cultural del país, a través del desarrollo productivo, innovador, incluyente y sostenible del sector artesanal y por su capacidad de mejorar las condiciones de vida de los artesanos, con un propósito continuo de innovación tecnológica, rentabilidad, desarrollo social y sostenibilidad para generar valor agregado y satisfacción en las soluciones que entregamos a nuestros clientes, se compromete a través de un sistema de gestión de seguridad de la información (SGSI) a:

- Implementar los controles necesarios que permitan proteger la información buscando mantener su confidencialidad, integridad y disponibilidad, para minimizar el riesgo, maximizar las oportunidades, responder a las necesidades de los grupos de interés y asegurar la continuidad del negocio.
- Impulsar una cultura interna en seguridad de la Información, a través del desarrollo de programas y planes de divulgación, capacitación, entrenamiento y concienciación
- Proteger la información generada, procesada, transmitida o resguardada por los procesos del negocio, aplicando controles de acuerdo con la clasificación de su información.
- Asegurar la disponibilidad de sus procesos de negocio y la continuidad de su operación de acuerdo con el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de sus obligaciones legales, regulatorias y contractuales establecidas.
- Asegurar los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de seguridad de la información.
- Promover una mejora continua de su sistema de gestión de seguridad de la información.

Ana María Fries Martínez
Gerente General

Junio de 2020

Carrera 2 # 18 A 58 Conmutador: (57) (1) 2861766 - (57) (1) 5550326 /27 /28 /29
www.artesaniasdecolombia.com.co Email: artesanias@artesaniasdecolombia.com.co
Bogotá, D.C. - Colombia
artesanías de colombia

Las políticas específicas se desarrollan teniendo en cuenta los dominios y los controles definidos en el Anexo A de la norma y la declaración de aplicabilidad, como se puede observar en la siguiente tabla:

Dominio	Objetivo de control
Políticas de seguridad de la información.	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
Organización de la seguridad de la información.	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
Seguridad de los recursos humanos	Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran.
Gestión de activos.	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
Control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.
Criptografía	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
Seguridad física y del entorno.	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
Seguridad de las operaciones.	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Seguridad de las comunicaciones	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
Adquisición, desarrollo y mantenimiento de sistemas.	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
Relaciones con los proveedores	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

Gestión de incidentes de seguridad de la Información.	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Aspectos de seguridad de la información de la gestión de continuidad de negocio.	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
Cumplimiento.	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Fuente: NTC/ISO 27001:2013.

9. AUTORIDADES Y ROLES DE SEGURIDAD DE LA INFORMACIÓN

Para asegurar el adecuado entendimiento de cada una de las políticas, a continuación se presentan las autoridades y los roles establecidos en el modelo de Seguridad de la información adoptado por la entidad e insumo para la definición de cada uno de los lineamientos:

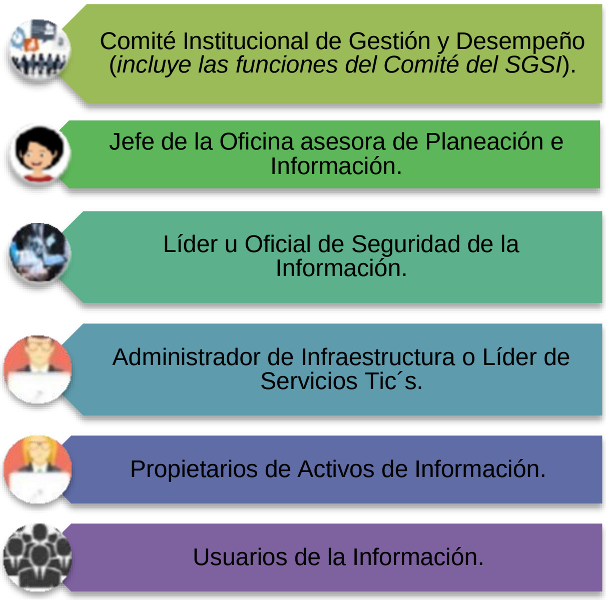


Ilustración 1. Autoridades y Roles de seguridad de la información de AdC

10. (A.5) POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

10.1 (A.5.1) ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Dominio/Control: A.5.1 Políticas para la Seguridad de la Información.

Objetivo: brindar orientación y soporte por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

Alcance: se debe definir un conjunto de políticas para la Seguridad de la Información, aprobada por la dirección, publicadas y comunicadas a los servidores públicos, contratistas, proveedores, pasantes y terceros.

Lineamientos: se debe dar cumplimiento a los siguientes lineamientos

10.1.1 (A.5.1.1) Políticas para la seguridad de la información

Las políticas de Seguridad y Privacidad de la Información de AdC, están relacionadas con la información o datos que se encuentran en los recursos tecnológicos, humanos y físicos, que manejan, administran y custodian los servidores públicos, contratistas, proveedores, pasantes y terceros.

Las políticas definidas a continuación se encuentran estructuradas y orientadas con base en cada dominio o control del Anexo A de la NTC ISO 27001:2013, y están alineadas con las prácticas de gestión de la NTC ISO 27002:2015.

10.1.2 (A.5.1.2) Revisión de las políticas para la seguridad de la información

a. La definición, actualización y mantenimiento del documento de Políticas de Seguridad y Privacidad de la Información de AdC, es responsabilidad del Líder u Oficial de Seguridad de Información quien debe revisar las políticas al menos una vez al año o cuando ocurran cambios significativos para asegurar su conveniencia, adecuación y eficacia continua; con la debida aprobación del responsable del Sistema Integrado de Gestión o quien haga sus veces y deberá seguir los lineamientos definidos en el procedimiento de control de documentos.

En las revisiones periódicas se debe tener en cuenta factores como:

- Prioridades de la Entidad.
- Costos e impacto de los controles a implementar por la Entidad.
- Incidentes de Seguridad de Información reportados.
- Nuevas vulnerabilidades detectadas.
- Cambios en los requerimientos regulatorios y/o legales.
- Cambios en la infraestructura tecnológica de la Entidad.
- Cambios en los objetivos del Sistema de Gestión de Seguridad de la Información "SGSI".
- Cambios en los objetivos de la Entidad entre otros.

10.2 (A.6) ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

10.2.1 (A.6.1) ORGANIZACIÓN INTERNA

Dominio/ Control: A.6.1 Organización Interna.

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la Seguridad de la Información dentro de la organización.

Alcance: La presente Política se alinea con el alcance de la implementación del Sistema de Gestión de Seguridad de la Información "SGSI" en AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. La oficina de planeación e información, a través del Oficial de Seguridad de la Información o quien haga sus veces, liderará la implementación del Sistema de Gestión de Seguridad de la Información "SGSI" en los siguientes procesos de la Entidad:

- Estratégicos.
- Misionales.
- Apoyo.
- Evaluación y Control.

b. La oficina de planeación e información, define en el Manual del Sistema de Gestión de Seguridad de Información “SGSI” los roles y responsabilidades.

c. La Entidad deberá mantener contacto con las autoridades pertinentes y los grupos de interés especiales tales como: Comando Conjunto Cibernético, Colcert, Policía Nacional, Profesionales Especializados en Seguridad, entre otros.

d. Todos los nuevos proyectos que se planteen ejecutar en la Entidad, independientemente de su naturaleza deberán contemplar los requisitos de Seguridad de la Información.

10.2.2 (A.6.2) POLÍTICA EN DISPOSITIVOS MÓVILES Y TELETRABAJO

Dominio/ Control: A.6.2.1 Política para Dispositivos Móviles

Objetivo: Garantizar la seguridad en el uso de los dispositivos móviles.

Alcance: La presente política aplica a todos los servidores públicos, contratistas, proveedores, pasantes y terceros o que, por su rol, hagan uso de dispositivos móviles en la entidad.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. La oficina de tecnologías de la información efectuará labores de monitoreo tanto a los dispositivos móviles propios de la Entidad como a los personales conectados a la red de AdC (cuando a ello haya lugar) con el objeto de adoptar los mecanismos de protección de la información y aplicar las medidas correctivas cuando se requieran.

b. La oficina de tecnologías de la información debe establecer las configuraciones definidas para el manejo tanto de los dispositivos móviles propios de la Entidad, como de aquellos que sean personales y se encuentren conectados en la red de AdC, siguiendo para ello las reglas generales de la guía para el uso aceptable de activos previamente adoptada.

c. Todos los usuarios que tengan autorizado el uso de dispositivos móviles personales, deben cumplir con las reglas generales establecidas en la Guía para el uso aceptable de activos.

d. Para agregar un dispositivo móvil personal a la red de AdC, debe contar con:

- El sistema operativo licenciado y actualizado (parchado).
- El antivirus licenciado y actualizado.
- La ofimática o aplicaciones necesarias para su gestión licenciadas.

NOTA: De no contener lo anterior el servidor público, contratista, proveedor, pasante y terceros se hace responsable por los incidentes que este riesgo genera a la entidad.

e. No se permite el ingreso a la entidad ni el acceso a la red de AdC, de equipos personales de escritorio

f. No es permitido instalar aplicaciones institucionales (sin autorización) en equipos personales móviles.

g. Aquellos equipos móviles personales que se encuentren conectados a la red de la entidad y estos no sean avalados y autorizados por la oficina de tecnología de la información serán catalogados como: **“Equipos NO autorizados**” y se podrá considerar como un incumplimiento a las Políticas de Seguridad y Privacidad de la Información definidas por la entidad.

h. Los equipos móviles personales, no tienen soporte de la Mesa de Ayuda por fallas que en ellos se presenten.

10.2.2 (A.6.2.2) POLÍTICA DE TELETRABAJO

Dominio/ Control: A.6.2.2 Teletrabajo.

Objetivo: Establecer los lineamientos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza Teletrabajo.

Alcance: La presente Política aplica para todos los Servidores Públicos o contratistas que laboren bajo la modalidad de Teletrabajo.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

AdC establece los siguientes lineamientos, en el marco de la Ley 1221 de 2008 "Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones":

AdC como Empleador debe:

a. Suministrar a los Teletrabajadores equipos de trabajo para la ejecución de sus obligaciones y/o funciones (cuando a ello haya lugar) o autorizar la utilización de equipos personales para el Teletrabajo, siempre y cuando se cumpla y acepten los mecanismos y medidas de Seguridad de Información definidos por la Entidad.

b. La oficina de tecnologías de la información y comunicación, no prestará ningún tipo de soporte por fallos de manejo en los equipos personales, que no estén relacionados con los servicios a través de los cuales accede al teletrabajo. (ejemplo: No – Ofimática, antivirus, actualizaciones, lentitud del equipo. Si – Uso de la VPN, Google Drive, Aplicaciones corporativas a las cuales va a acceder)

c. Será responsable del licenciamiento del Software de los equipos suministrados a los Teletrabajadores para su gestión.

d. Dar a conocer a los Teletrabajadores los lineamientos impartidos a través de la presente Política y con ello los riesgos de su proceso que se derivan por el uso de los equipos tecnológicos para la Seguridad de la información de la Entidad.

e. Definir los tipos de usuarios que dispondrán de modalidad de Teletrabajo y los permisos de acceso remoto pertinentes.

f. Establecer procedimientos para la solicitud y autorización del Teletrabajo.

g. Establecer un procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.

h. Establecer un compromiso por parte del Teletrabajador (en el documento que defina la entidad), frente al cumplimiento de los lineamientos adoptados a través de la presente política, así como en lo relacionado al uso exclusivo del equipo (asignado por la

Entidad o Personales), que se destine para la ejecución de sus obligaciones y/o funciones (según sea el caso), aceptando y cumpliendo para tales efectos con las medidas de seguridad de la información implementadas por la entidad.

i. Identificar los derechos y obligaciones de cada una de las partes que intervienen en el Teletrabajo.

j. La oficina de tecnologías de la información llevará el seguimiento de las conexiones remotas a los servicios relacionados con el Teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.

El Teletrabajador de AdC, debe:

a. No podrá instalar software que no esté autorizado. (Ver política uso aceptable de los activos).

b. Deben cumplir con las Políticas de Seguridad y Privacidad de Información definidas y establecidas por la Entidad.

c. Deben cumplir con las reglas generales establecidas en la Guía para el uso aceptable de activos.

d. No debe almacenar información Sensible o Confidencial en los equipos asignados por la entidad o personales sin que esta información esté cifrada para efectos de Seguridad.

e. Si los equipos para la ejecución de las funciones son personales se debe:

- Tener Sistema Operativo Licenciado y actualizado (parchado).
- Tener antivirus licenciado y actualizado.
- Tener la ofimática o aplicaciones necesarias para su gestión licenciadas.
- Mantener las aplicaciones actualizadas.
- Utilizar el control de acceso definido por la entidad con sus correspondientes permisos.
- Mantener configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.).
- Parametrizar el bloqueo automático por inactividad y en lo posible, utilizar un cifrado de disco.

- No facilitar a otra persona las credenciales de acceso o el perfil de acceso a los servicios o recursos tecnológicos de Adc.

f. Los equipos asignados por la entidad o personales, no deben dejarse desatendidos

g. Para el transporte de equipos portátiles entre la oficina y el lugar o lugares en que se ejecuten las funciones de Teletrabajo, es necesario disponer de un maletín que ofrezca buena resistencia a caídas, golpes, aplastamiento, derrame de líquidos u otro riesgo al que se encuentre expuesto el equipo.

h. Guardar bajo llave en el sitio o sitios en los que se ejecuten las funciones de Teletrabajo, el dispositivo mientras no se utiliza.

i. Establecer medidas de seguridad de la información, con el objeto de evitar el acceso no autorizado a la información institucional.

j. Manejar cuentas de usuario independientes si el equipo para la ejecución de las funciones de Teletrabajo es personal.

k. No utilizar en los equipos portátiles asignado por la entidad o personales conexiones poco confiables como:(Wi-Fi abiertas, redes Públicas de hoteles, bibliotecas, locutorios, aeropuertos, entre otros) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS).

l. Verificar que en el acceso a los servidores institucionales se utilicen certificados reconocidos y que la figura del “candado” de la conexión SSL, nos permite identificar que no existan posibles peligros o errores.

m. Utilizar contraseñas seguras siguiendo los lineamientos de la Política de control de acceso de AdC.

n. Borrar el historial de navegación, las cookies y otros datos del navegador web en el equipo asignado por la Entidad o personal.

o. No debe usar el cuadro de diálogo en el que se sugiere recordar contraseña por Políticas de seguridad de la Información en el equipo asignado por la Entidad o personal.

p. Debe cerrar las conexiones con servidores y páginas web mediante la opción "desconectar" o "cerrar sesión" al finalizar su labor en el equipo asignado por la Entidad o personal.

q. Debe eliminar la información temporal alojada en carpeta de descargas, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del equipo asignado por la Entidad o personal.

r. Solicitar a la mesa de ayuda de la entidad, cuando sea necesario, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en el equipo asignado por la entidad o personal con el que se ejecuten las labores de Teletrabajo, previa autorización cuando sea el caso.

s. Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el equipo asignado por la entidad o personal.

t. En lo que respecta a la información que se encuentre contenida en medios físicos, los teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de Seguridad de la Información establecidos por la Entidad y que a continuación se relacionan:

- Almacenar los documentos bajo llave mientras no se estén utilizando.
- No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de Teletrabajo.

10.3 (A.7) POLÍTICA DE SEGURIDAD EN LOS RECURSOS HUMANOS

Dominio/Control: A.7. Seguridad del Recurso Humano.

Objetivo: Asegurar que los funcionarios y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.

Alcance: La presente política establece que todos los servidores públicos, contratistas, proveedores, pasantes y terceros, deben dar cumplimiento a las Políticas de Seguridad y Privacidad de la información de AdC.

Lineamientos:

Se debe dar cumplimiento a los siguientes lineamientos:

AdC, reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con personal calificado, deberá garantizar que la vinculación de los candidatos, aspirantes, contratistas, proveedores y terceros cumplan con los procesos de verificación necesarios, el cual estará orientado al perfil, a las funciones y/u obligaciones que deben desempeñar para desarrollar su labor.

10.3.1 (A.7.1) ANTES DE LA VINCULACIÓN

Asegurar que los candidatos, aspirantes, contratistas y proveedores comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran:

a. El Grupo de Gestión de Talento Humano y Gestión Contractual de acuerdo a su competencia, deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por los candidatos o aspirantes a ocupar un cargo en AdC, antes de su vinculación definitiva.

b. El Grupo de Gestión de Talento Humano debe convocar a los Servidores Públicos de la Entidad, para que asistan a las charlas inducción y reinducción donde se darán a conocer las Políticas de Seguridad y Privacidad de la Información.

c. Se debe incorporar dentro de las minutas contractuales, cláusulas referentes a:

- Estricto cumplimiento de las Políticas de Seguridad y Privacidad de la Información definida por la Entidad.
- Confidencialidad de la Información.
- Cláusulas de Tratamiento de Datos Personales.

d. El Grupo de Gestión de Talento Humano y Gestión Contractual de acuerdo a su competencia, debe realizar verificaciones de los antecedentes de todos los candidatos o aspirantes, se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes y deben ser proporcionales a los requisitos de la entidad, a la clasificación de la información a que va a tener acceso, y a los riesgos percibidos.

e. El personal provisto por terceros, debe garantizar el cumplimiento de los acuerdos y/o Cláusulas de Confidencialidad y de aceptación de las Políticas de Seguridad de la Información de la Entidad antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica de la misma.

f. En el Manual de Funciones de la Entidad, se deberá incluir un capítulo del estricto cumplimiento a las Políticas de Seguridad y Privacidad de la información de la Entidad por parte de los Servidores Públicos.

10.3.2 (A.7.2) DURANTE DE LA VINCULACIÓN

Asegurar que todos los servidores públicos, contratistas, proveedores, pasantes y terceros, tomen conciencia de sus responsabilidades de Seguridad y Privacidad de la información, considerando el cumplimiento de los siguientes lineamientos:

a. El Grupo de Gestión de Talento Humano, deberá notificar cualquier novedad del personal en el que se encuentre en situaciones administrativas tales como: (licencias, vacaciones, traslado, retiro, entre otras); para que la oficina de tecnologías de la información y las áreas que administran los aplicativos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.

b. El Grupo de Gestión Contractual, deberá notificar cualquier novedad de contratistas, proveedores, pasantes y terceros tales como: (ceder contrato, terminación bilateral, terminación unilateral, entre otras), referente a su vinculación o relación comercial con la entidad para que la oficina de tecnologías de la información y las áreas que administran los aplicativos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados.

c. La oficina asesora de planeación e información, a través del líder de seguridad o quien haga sus veces, deberá diseñar y ejecutar de manera periódica (mínimo una vez al año) un Plan de Cultura y Sensibilización de la Información para todos los Servidores Públicos, Contratistas, Proveedores, pasantes y Terceros, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

d. Se debe contar con un proceso formal y comunicado para emprender acciones contra servidores públicos, contratistas, proveedores, pasantes y terceros que hayan cometido una violación a la Seguridad y Privacidad de la Información de la Entidad.

e. Si se realizan cambios en las funciones y/o actividades en los servidores públicos, contratistas, proveedores, pasantes y terceros, estos deberán ser notificados a la oficina de tecnologías de la información y/o Líder de Seguridad de la Información, para que con las instrucciones del líder del proceso se apliquen los ajustes necesarios para el uso de los servicios tecnológicos.

f. Se debe sensibilizar y divulgar a través de los medios establecidos por la entidad sobre la Seguridad y Privacidad de la Información, a los servidores públicos, contratistas, proveedores, pasantes y terceros, los cuales deben participar activamente en los Programas o Planes de Cultura y Sensibilización en Seguridad de la Información desarrollados por la Oficina de Tecnologías de Información, y de acuerdo al contenido debe ser interiorizado y aplicado según corresponda su rol y responsabilidad dentro de la Entidad.

g. El contenido de los Programas o Planes de Cultura y Sensibilización de Seguridad de la Información deben enmarcarse en tres (3) fases:

- Diseño. Deben ser diseñados teniendo en cuenta la misión de la entidad, identificación de las necesidades y prioridades (verificación de incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.

- Desarrollo. Elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de Seguridad y este debe ser sometido a aprobación por la Alta Dirección, antes de la puesta en marcha.

- Implementación. Socializar el programa o Plan de Cultura Sensibilización de Seguridad de la Información de la Entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del Programa o Plan.

10.3.3 (A.7.3) TERMINACIÓN Y CAMBIO DE EMPLEO

a. Los servidores públicos, contratistas, proveedores, pasantes y terceros, deberán mantener la confidencialidad de la información después de su vínculo laboral o relación comercial con la entidad, de acuerdo a lo establecido en el manual de funciones y/o obligaciones contractuales.

b. La oficina de tecnologías de la información y las áreas que administren las aplicaciones, deberán suspender los servicios de TI a los servidores públicos, contratistas, proveedores, pasantes y terceros que no tengan ningún tipo de vinculación con la Entidad, siempre y cuando este sea informado por el Grupo de Gestión de Talento Humano y el Grupo de Gestión Contractual.

c. Los servidores públicos, contratistas, proveedores, pasantes y terceros, deberán entregar los elementos tales como: (computador, discos duros, tabletas, GPS, archivo físico y digital, entre otros) para que la entidad le genere paz y salvo.

10.4 (A.8) GESTIÓN DE GESTIÓN DE ACTIVOS

10.4.1 (A.8.1) RESPONSABILIDAD POR LOS ACTIVOS

Dominio/Control: A.8.1. Responsabilidad por los activos.

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

Alcance: La presente política aplica para todos los servidores públicos, contratistas, proveedores, pasantes y terceros o que, por su rol, tengan bajo su propiedad o custodia, activos de información.

Lineamientos:

Se debe dar cumplimiento a los siguientes lineamientos:

10.4.1.1 (A.8.1.1) Inventario de activos

El Líder u Oficial de Seguridad de la Información o quien haga sus veces, es el encargado de llevar a cabo funciones de orientación y apoyo en cada uno de los Procesos Institucionales a través de las actividades para la identificación de activos de información, con el objeto de contribuir a que los inventarios de activos de cada una de las dependencias de AdC, se encuentren en las Tablas de Retención Documental y cumplir con los criterios establecidos en el procedimiento de Identificación, Valoración y Clasificación de Activos de Información, asegurando que:

a. Toda la información deberá ser clasificada por:

- Su nivel de criticidad.
- Su valor.
- Disposiciones de normativa legal.
- Las indicaciones de los propietarios de la información como por la Entidad.

b. La Matriz de identificación y clasificación de activos de información debe permanecer en un repositorio seguro con acceso restringido.

c. La Matriz de identificación y clasificación de activos de información se debe actualizar por lo menos una vez al año y/o cuando se presenten:

- Cambios en la tabla de retención documental.
- Retiro de activos de información.
- Adquisiciones de nuevos activos de información.

d. Mantener actualizado el inventario de los activos de información tecnológicos de la entidad tales como (redes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, portátiles y licencias de software), así como aires acondicionados, generadores de energía, unidades de potencia (UPS).

e. Los activos de información deberán estar publicados de acuerdo a la legislación actual vigente.

f. Los activos de información tanto físicos como digitales deberán estar rotulados de acuerdo a la Guía de Clasificación de información definida por la Entidad.

10.4.1.2 (A.8.1.2) Propiedad de los activos de información

Quien ejerza las funciones de propietario de activos de información en AdC deberá:

a. Velar porque todos los activos de información bajo su propiedad se encuentren debidamente inventariados.

b. La Entidad, deberá identificar cuáles son los propietarios de la información y asignar responsabilidades para:

- Definición de controles para la protección de los activos de Información.
- Mantenimiento de los controles definidos para la protección de los activos de Información.
- Seguimiento y/o monitoreo de los custodios de los activos de Información para la verificación de la aplicación de los controles definidos.

c. Verificar que los activos de información sean clasificados y protegidos de acuerdo a:

- Su nivel de criticidad.
- Su valor.
- Disposiciones de normativa legal.

d. Revisar al menos una vez al año o cuando ocurra un cambio significativo, las restricciones y clasificaciones de acceso a los activos de información.

e. Verificar que los procesos de eliminación o destrucción no permitan la exposición de los activos de información a terceros.

10.4.1.3 (A.8.1.3) Uso aceptable de los activos de información

a. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que por su rol, tengan bajo su propiedad o custodia, activos de información de la Entidad, deben acatar y dar estricto cumplimiento a lo prescrito en la Guía de Uso Aceptable de los Activos de Información.

10.4.1.4 (A.8.1.4) Devolución de los activos de información

a. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros, deben hacer devolución del activo de información bajo su responsabilidad, una vez finalizado el vínculo con la Entidad.

b. Una vez finalizado el vínculo con la Entidad, el Jefe de Área o Supervisor del Contrato (según sea el caso) deberá solicitar a la Mesa de Ayuda, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en los equipos asignados para la ejecución de sus funciones u obligaciones contractuales, previo a la generación del backup de la Información que allí se aloje.

c. El Jefe de Área o Supervisor del Contrato (según sea el caso), debe asegurarse que los equipos que se encuentren bajo su custodia y estos sean:

- Devueltos al almacén de la Entidad.
- Reasignado a un servidor público, contratista, pasante, proveedor o tercero de la Entidad.
- Traspasados a otra Área, Dependencia o Seccional de la Entidad.
- Destruidos o dar de baja.
- Donados a Terceros.

10.4.2 (A.8.2) CLASIFICACIÓN DE LA INFORMACIÓN

Dominio/Control: A.8.2. Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización

Alcance: La presente política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que, por su rol, tengan bajo su propiedad o custodia, activos de información.

Lineamientos:

Se debe dar cumplimiento a los siguientes lineamientos:

10.4.2.1 (A.8.2.1) Clasificación de la información

a. Los únicos niveles de clasificación de información establecidos en AdC son: Publica, Uso Interno, Confidencial (Sensible) y Reservada por tanto, el dueño del proceso está obligado a clasificar y dar el tratamiento adecuado a la información de acuerdo a estos niveles y siguiendo los lineamientos de la Guía de Clasificación y Rotulado de Información de AdC.

b. Los propietarios de los activos de Información, están obligados a clasificar y dar tratamiento adecuado a la misma, de acuerdo a los niveles definidos en la Guía de Clasificación y Rotulación de la Entidad.

10.4.2.2 (A.8.2.2) Etiquetado de la información

a. Cada activo debe poseer un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico, electrónico y digital.

10.4.2.3 (A.8.2.3) Manejo de activos de información

a. Para el manejo, procesamiento, almacenamiento y comunicación de la información se debe considerar los niveles de clasificación definidos en la Guía de Clasificación y Rotulación de la Entidad.

b. La eliminación y destrucción de la información debe realizarse de acuerdo a su nivel de clasificación y siguiendo los lineamientos de la Guía de Clasificación y Rotulado de Información de AdC.

c. Teniendo en cuenta que la Integridad es un principio fundamental de la seguridad de la información, se deben cumplir con:

- En lo que respecta a todas las aplicaciones de la Entidad, se deben implementar mecanismos cuyo objeto sea el de propender por la Integridad del Activo de información con base en el nivel de clasificación y el nivel de evaluación de Riesgo identificado.
- La oficina de tecnologías de la información de la Entidad, será la única dependencia autorizada para realizar copia de Seguridad del Software Original.

- El software proporcionado por la Entidad, no puede ser copiado o suministrado a terceros.

10.4.3 (A.8.3) MANEJO DE MEDIOS

Dominio/Control: A.8.3. Manejo de Medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

Alcance: La presente política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que, por su rol, tengan bajo su propiedad o custodia, activos de información.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.4.3.1 (A.8.3.1) Gestión de medios removibles

a. Cualquier dispositivo de almacenamiento de información de propiedad de la Entidad, se constituye en un activo de información, por tanto, el ingreso, uso, movilización y salida, debe ser previamente autorizado por la (s) dependencia (s) competente (s).

b. Se debe mantener un inventario actualizado de los dispositivos de almacenamiento de información removible de la entidad como (Cintas de Backup, Discos Duros, USB, GPS, entre otros) y de sus propietarios.

c. Los propietarios y custodios de los medios removibles, deben asegurarse que éstos no queden desatendidos debido a que pueden ser susceptibles a pérdida o robo.

d. La protección a los medios debe hacerse de acuerdo al nivel de clasificación definidos por la entidad para la información contenida en los mismos.

e. El uso de dispositivos de almacenamiento personales como (USB, DISCO DUROS EXTERNOS, ENTRE OTROS) están prohibidos.

f. Todos los medios de almacenamiento removibles, deben ser almacenados en un ambiente seguro de acuerdo a las especificaciones de los fabricantes.

g. Si ya no se requiere de la información contenida en los medios removibles de la Entidad, se deberá aplicar técnicas de borrado seguro para que estos puedan ser reutilizados.

10.4.3.2 (A.8.3.2) Disposición de los medios

a. Una vez terminado el ciclo de vida útil de un determinado medio de almacenamiento, la información allí contenida, debe ser eliminada de manera segura de acuerdo con los procedimientos formales previamente establecidos por la Entidad, previo a la generación de backup de la información que allí se contenga.

b. Se debe tener en cuenta el procedimiento para la disposición de dispositivos tecnológicos RAES para los equipos y medios de almacenamiento que se den de baja.

c. La Entidad debe asegurarse que se implemente los controles establecidos para la disposición segura de medios definidas por la Entidad, cuando se vayan a:

- Destruidos o dar de baja.
- Donados a Terceros.

d. Para la eliminación de medios de almacenamiento se debe generar un registro mediante acta con el fin de mantener registros para efectos de auditorías.

10.4.3.3 (A.8.3.3) Transferencia de medios físicos

a. El transporte de los medios de almacenamiento de la Entidad, debe darse de acuerdo a la clasificación de la información contenida en éstos, para ello se deben:

- Utilizar servicios de mensajería confiables.
- Verificar los tipos de monitoreo para la transferencia de medios físicos.
- Verificar si se realizan técnicas de embalaje.
- Llevar un registro correspondiente de los medios físicos que son transportados.

10.5 A.9 POLÍTICA DE CONTROL DE ACCESO

10.5.1 A.9.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO

Dominio/Control: A.9.1 Política de control de Acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. Los Sistemas de Información de la Entidad, debe contar con mecanismos para el control de acceso lógico. Estos mecanismos se deberán revisar con una periodicidad de dos (2) veces al año.

b. Establecer medidas de control de acceso para los servidores públicos, contratistas, pasantes, proveedores y terceros, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de Red, Sistemas de Información, Bases de Datos y Servicios de TI de acuerdo con los perfiles y cargos establecidos en la Entidad.

c. La Entidad, proporcionará a los servidores públicos, contratistas, pasantes, proveedores y terceros, los recursos tecnológicos necesarios para que puedan desempeñar las funciones de una manera eficaz.

d. No se permite conectar o instalar, de manera cableada o inalámbrica a la red LAN de la Entidad, cualquier dispositivo fijo o móvil como: (computadores de escritorio, portátiles, Tablet, enrutadores, switches, agendas electrónicas, Smartphone, Access point, amplificadores de señal, entre otros) que no sean autorizados por la oficina de tecnologías de la información y el Líder de Seguridad de la Información.

e. El acceso a la red interna por parte de un proveedor, debe estar autorizada por la oficina de tecnologías de la información y el Líder de Seguridad de la Información mediante los mecanismos definidos por la Entidad.

f. El tiempo de inactividad de una sesión de usuario, debe activarse de acuerdo a la Política del Directorio activo.

g. Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador), se deben cambiar de acuerdo al análisis previo realizado por la oficina de tecnologías de la información y el Oficial de Seguridad de la Información; y para ello se debe convocar a Comité de Cambios donde se aprobará y se programará el cambio.

h. Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador), se deben proteger y almacenar bajo la custodia del Jefe de la Oficina de Tecnología de Información.

i. El Grupo de Gestión de Talento Humano y Gestión Contractual, deberán informar a los Administradores de los Sistemas de Información y/o Aplicaciones de la Entidad, lo referente a novedades que surjan para los S servidores públicos, contratistas, pasantes, proveedores y terceros, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.

j. Los controles de autenticación deben ser confiables, para lo cual la entidad adelantará los mecanismos o procedimientos que ello amerite.

k. Quien (es) ejecute(n) el rol de Administrador de programas fuentes debe(n):

- Tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo.
- Llevar un registro actualizado de todos los programas fuentes en uso, indicando entre otros, el nombre del programa, programador, analista responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Restringir el acceso a los códigos fuente de los programas, asegurándose de que solamente los ingenieros desarrolladores tengan acceso.
- Mantener los códigos fuente de los programas en el servidor o repositorio de fuentes.

- Asegurarse de que el código y las bibliotecas fuentes del programa sean manejadas con los procedimientos establecidos.
- Realizar el mantenimiento y copiado de las bibliotecas fuentes del programa de acuerdo con el procedimiento de control de cambios.
- Asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

10.5.2 A.9.2 POLÍTICA DE GESTIÓN DE ACCESO A USUARIOS

Dominio/ Control: A.9.2. Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. AdC establece los privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos y servicios tecnológicos y los sistemas de información. Así mismo, velará porque los servidores públicos, contratistas, pasantes, proveedores y terceros tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada con procedimientos establecidos para tal fin.

b. Quien(es) ejecute (n) el rol de Líder de Servicios Tic´s o quien haga de sus veces, debe (n):

- Dar cumplimiento a la aprobación o rechazo de los permisos de conexión remota o VPN, previamente otorgado por la oficina de tecnologías de la información de la Entidad o quien haga sus veces, En lo que respecta a la solicitud de acceso lógico que efectúen los servidores públicos, contratistas, pasantes, proveedores y terceros, esta debe ir respaldada, soportada y avalada por el Jefe inmediato o Supervisor del contrato según sea el caso.

- Asegurar que las redes inalámbricas cuenten con métodos de autenticación que eviten accesos no autorizados.
- Velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.
- Realizar una verificación de los controles de acceso de los servidores públicos, contratistas, pasantes, proveedores y terceros en la periodicidad que se establezca para ello, a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la des habilitación o suspensión de aquellos usuarios que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite.
- Asignar los privilegios a los usuarios de acuerdo con los roles y responsabilidades, estos privilegios se extenderán sólo cuando sea necesario y deben contar con autorización del Jefe o Supervisor del Contrato y visto bueno de la oficina de tecnología de la información y el Líder u Oficial de Seguridad de Información.
- Cancelar los derechos de acceso a la información a todos los servidores públicos, contratistas, pasantes, proveedores y terceros que no tengan vinculación con la Entidad.

c. El acceso a los recursos de red, serán controlados por medio de la creación de usuarios y password correspondientes, con el fin de prevenir el acceso no autorizado.

d. Los servidores públicos, contratistas, pasantes, proveedores y terceros de la Entidad, tendrán solamente acceso a los servicios de red y Sistemas de Información para los cuales fueron autorizados y que son necesarios para realizar sus funciones.

e. Los servidores públicos, contratistas, pasantes, proveedores y terceros de la Entidad, deben reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece en la herramienta de Mesa de Ayuda como incidente de Seguridad de Información.

10.5.3 A.9.3 POLÍTICA DE RESPONSABILIDAD DE LOS USUARIOS

Dominio/ Control: A.9.3 Responsabilidad de los usuarios

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

Alcance: La presente servidores públicos, contratistas, pasantes, proveedores y terceros o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros, deben bloquear el equipo en caso de ausentarse del puesto de trabajo, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.

b. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros, deben apagar el equipo una vez termine la jornada laboral, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.

c. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros bajo ningún motivo deberán prestar su usuario y contraseña para acceder al equipo y/o aplicaciones de la Entidad.

d. Es responsabilidad de los servidores públicos, contratistas, pasantes, proveedores y terceros, el buen manejo y uso de los recursos de la Entidad, así como de las claves que le han sido asignadas.

e. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros, que con ocasión a sus tareas u obligaciones con la Entidad, tengan acceso a los Sistemas de Información, deben utilizar el nombre de usuario válido del dominio AdC, asignándole para ello una contraseña que cumpla con las políticas de seguridad adoptadas por la entidad, la cual deberá ser personal e intransferible.

f. Para la creación de contraseñas seguras, los servidores públicos, contratistas, pasantes, proveedores y terceros, deben:

- Escoger contraseñas que sean difíciles de descifrar y que no contengan información relacionada con su trabajo o vida personal, por lo cual no se debe utilizar la siguiente información: Números de identificación personal, números de teléfono, nombres de los cónyuges, direcciones postales, nombres propios, lugares conocidos o términos técnicos.

- Combinar palabras (Mayúsculas o minúsculas), puntuación y números, de tal modo que arroje como resultado una contraseña alfanumérica con símbolos especiales.

- Transformar una palabra común utilizando un método específico.

- Crear acrónimos (siglas que forman una palabra).

- Crear contraseñas que contengan como mínimo 8 dígitos y cambiarla a intervalos de 30 días.

- Los intentos no exitosos de ingreso de la contraseña, después de un número de veces determinado y previamente establecido por la entidad, traerá consigo el bloqueo del usuario de manera inmediata para lo cual se deberá solicitar el desbloqueo a quien ejecute el rol de Administrador de control de acceso lógico.

g. Las contraseñas que sean suministradas a través de correo electrónico por quien ejecute el rol de administrador de un determinado Sistema, deben ser cambiadas de manera inmediata tan pronto como la misma sea recibida por parte de la persona a quien se le han asignado los permisos, siguiendo para ello con los protocolos de seguridad de la información y las buenas prácticas de uso de contraseña aludidas.

h. Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.

i. Si algún servidores públicos, contratistas, pasantes, proveedores y terceros, sospecha (n) de la pérdida de confidencialidad de alguna de sus claves, debe(n) notificar el evento o incidente de seguridad de la información (según sea el caso) a la mesa de ayuda de AdC, a fin de tomar las medidas pertinentes de cuidado de la información y supervisar la generación de nuevas credenciales siguiendo los lineamientos del Procedimiento Gestión de Incidentes de Seguridad de la Información de la Entidad.

10.5.4 A.9.4 POLÍTICA CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

AdC deberá asegurar, preservar y garantizar el control de acceso a los Sistemas y/o Aplicaciones Institucionales, para lo cual deberá dar cumplimiento a los siguientes parámetros de Seguridad:

a. El acceso a los Sistemas de Información y Servicios Tecnológicos de la Entidad, a través del uso de usuario de dominio AdC, debe estar restringido y delimitado a las tareas, funciones, responsabilidades u obligaciones que ejecuten los servidores públicos, contratistas, pasantes, proveedores y terceros de la Entidad.

b. El propietario de la aplicación y de la información, deberá identificar y documentar explícitamente la Sensibilidad o Confidencialidad de la Información contenida en los Sistemas Información y/o Aplicaciones de la Entidad.

c. Los propietarios de los activos de Información, deben autorizar los accesos a sus Sistemas de Información y/o Aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la Clasificación de la Información

d. No está permitido para ningún servidor público, contratista, pasante, proveedor y tercero, acceder a los Sistemas de Información y/o Aplicaciones para el cual no haya sido autorizado.

e. Quien(es) ejecute(n) el rol de Líder de Servicios Tic´s o quien haga de sus veces, debe (n):

- Asegurar que los grupos de servicios de información, usuarios y Sistemas de Información sean segmentados en redes.
- Establecer los controles de acceso a los ambientes de producción de los Sistemas de Información.
- Asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción de la Entidad.
- Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

- Asegurar que en lo que respecta a los Sistemas Operativos, Sistemas de Información y/o Aplicaciones de la Entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.
- Garantizar que los Sistemas de Información y/o Aplicaciones de la Entidad, tengan establecidos “Time Out” después de determinados minutos de inactividad previamente establecidos. Esto debe estar tanto para las Aplicaciones locales y web.
- En lo que respecta a la autorización y continuidad en el uso de los usuarios de los aplicativos, deberá ser responsabilidad de cada una de las Áreas, Dependencias y/o Procesos de la Entidad.

10.6 A.10 POLÍTICA DE CRIPTOGRAFÍA

10.6.1 A.10.1 Controles Criptográficos

Dominio/Control: A.10.1 Controles Criptográficos.

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

Alcance: La presente política aplica para todos los servidores públicos o contratistas de AdC que hagan uso de controles criptográficos, cuando se requiera.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. Quien(es) ejecute(n) el rol de Líder de Servicios Tic´s o quien haga de sus veces, debe (n):

- Con la participación de los dueños de los activos de información, identificar los Sistemas de Información y/o Aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos de los Sistemas de Información, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.).

- Documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y destrucción de las claves criptográficas y debe mantener un registro de actividad que evidencie su cumplimiento y permita su posterior revisión o auditoría.

b. Los aspectos importantes que se deben tener en cuenta para el uso de los controles criptográficos son:

- Para la Información Sensible y/o Confidencial de la Entidad.
- Para las líneas de comunicación por donde se almacena, procesa y transmite la información Confidencial.
- Las herramientas y mecanismos de cifrado definidas por la Entidad.
- Para el cumplimiento de los Requisitos legales.

c. Se debe realizar una gestión segura de todas las claves criptográficas, por parte de quienes requieran su uso, con el objeto de garantizar la eficacia de los controles criptográficos.

d. Cuando se utilicen mecanismos de cifrado simétrico o de clave privada (compartida), se debe garantizar la confidencialidad en el intercambio de las claves (por un canal seguro o cifradas mediante mecanismos de cifrado asimétrico).

e. Cuando se utilicen mecanismos de cifrado asimétricos o de clave pública/privada, se debe:

- En el intercambio de claves públicas, la autenticidad e integridad de las mismas deben quedar avaladas por una autoridad de certificación de confianza, bien sea interna (PKI interna) o externa.
- En el caso de uso de servicios criptográficos de terceros, los acuerdos de prestación de servicios deben cubrir aspectos de responsabilidad civil, fiabilidad y seguridad del servicio y tiempos de provisión.

f. Para los tokens de Seguridad suministrados a los Servidores Públicos y/o Contratistas, para realizar consulta, modificación, transmisión de información, pagos, entre otros fines:

- Se debe guardar en un lugar seguro bajo llave, libre de acceso al mismo por personal no autorizado.
- No se debe dejar desatendido cuando el usuario se encuentre ausente del puesto de trabajo.
- No se puede prestar el token ni suministrar la clave bajo ninguna circunstancia.
- No se debe utilizar fuera de las instalaciones de la Entidad.
- No se debe utilizar en horario no laboral sin previa autorización escrita del Jefe o Supervisor de Contrato.

- Si el token se bloquea por intentos fallidos por el uso del mismo se debe solicitar el desbloqueo a la Entidad “Administradora” del mismo, previo a solicitud en la Mesa de Ayuda de la oficina de tecnologías de la información, para autorizar el servicio remoto mediante aprobación del Líder u Oficial de Seguridad de la Información.

10.7 A.11 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Dominio/ Control: A.11.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Alcance: La presente política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que por su rol tengan acceso físico a las instalaciones y áreas seguras de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.7.1 A.11.1 ÁREAS SEGURAS

10.7.1.1 A.11.1.1 Perímetros de Seguridad Física

Las áreas y dependencias de AdC, deben encontrarse protegidas por controles físicos, monitoreados y supervisadas con circuito cerrado de cámaras. La Entidad se define las siguientes áreas seguras:

a. **Datacenter:** corresponde al centro de procesamiento de datos en donde se encuentran sistemas de información (aplicaciones, bases de datos, directorio activo, entre otros), los componentes de telecomunicaciones y los sistemas de almacenamiento (servidores físicos y virtuales).

b. **Centros de Cableado**: áreas que se usan para conectar los dispositivos de la red de área local (LAN) donde se encuentran paneles de conexión, Hubs de cableado, Switches, Router, Puentes, entre otros.

c. **Cuartos de Suministro**: áreas en donde se ubican los servicios de suministro como: las UPS y la planta eléctrica.

d. **Archivo Físico Central:** áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico entre otros que son transferidos por las diferentes oficinas.

e. **Archivo Físico de Gestión:** Hace referencia a aquella documentación todavía en trámite que conservan las oficinas, así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa por las mismas oficinas, aplicando para ello lo dispuesto en las tablas de retención documental.

f. **Oficinas:** todas aquellas dependencias y áreas de la Entidad, que por sus competencias funcionales manejan información Sensible y Confidencial, serán consideradas “Áreas Seguras”, para lo cual deben adoptarse los mecanismos tendientes para asegurar dicha información.

10.7.1.2 A.11.1.2 Controles de Acceso Físico

a. Impedir que aquellas áreas cuyas ventanas dan al exterior por su ubicación, permiten de alguna manera (al menos mínima) la visibilidad hacia el interior de la Entidad, para lo cual es necesario que las mismas deben estar cerradas con llave.

b. Implementar los controles de seguridad de las áreas seguras de acuerdo con el nivel de protección que se requiera.

c. Los privilegios de acceso a las áreas seguras de AdC, son definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:

- Profesionales que trabajan regularmente en las áreas seguras.
- Profesional de soporte que requiere acceso periódico.
- Visitantes (servidores públicos, contratistas, pasantes, proveedores y terceros) que requieren acceder esporádicamente.

d. Los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso, firmar el respectivo control y portar un documento que demuestre y en todo caso acredite la calidad en la que actúa para efectuar dicho ingreso. En este tipo de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.

- El acceso al Datacenter está restringido y su ingreso es únicamente para el personal autorizado por AdC.

- Para acceder a los Centros de Cableado, se debe diligenciar la bitácora de ingreso y salida. Esto debe aplicarse para los servidores públicos, contratistas, proveedores y terceros autorizados por la oficina de tecnologías de la información.

- Para el ingreso de los visitantes, en las áreas seguras se debe llevar un registro de la fecha y la hora de entrada y salida, profesional que autoriza, dependencia o entidad a la que pertenece y actividad realizada, entre otros que sean requeridos para cada caso en particular.

- Las actualizaciones a los derechos de acceso, pueden ser efectuadas cuando ello así se requiera por parte de cada profesional u oficina encargada del área segura, para lo cual, si es del caso, se revocarán aquellos permisos que ya no sean necesarios.

10.7.1.3 A.11.1.3 Seguridad de oficinas, recintos e instalaciones

Con el propósito de mantener la Confidencialidad, Integridad y Disponibilidad de la Información en las oficinas, recintos e instalaciones, es necesario establecer y dar cumplimiento a las siguientes directrices de Seguridad:

a. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros deben presentar su carné o documento de identificación, según sea el caso, para el ingreso a las instalaciones de la Entidad.

b. Todos los servidores públicos, contratistas, pasantes, proveedores, terceros y visitantes deben portar visiblemente la escarapela, carne o documento que los acredite como tal, mientras se encuentren en las instalaciones de la Entidad.

c. Todo el personal que ingrese o salga de las instalaciones de la Entidad independientemente de su calidad, deberá registrar en la bitácora de vigilancia, el ingreso y salida de los dispositivos tecnológicos institucionales o personales.

d. Todo visitante debe notificar y registrarse en la recepción, la oficina o área a la que se dirige y su ingreso debe estar previamente autorizado.

e. Todas las oficinas de AdC que procesen, almacenen y/o gestionen información reservada o sensible deben implementar y adoptar las medidas tendientes a asegurar dicha información.

f. Para aquellas oficinas cuyo acceso físico, se de a través de puertas, es deber del Jefe de oficina correspondiente, salvaguardar las llaves de esta y asegurar una copia en un lugar diferente y seguro.

g. Los materiales o combustibles, deben ser almacenados de manera segura a una distancia prudente de las áreas de procesamiento y almacenamiento de información.

h. Los suministros de papelería no deben almacenarse en Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión).

i. En las Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión), no se debe utilizar como bodega.

10.7.1.4 A.11.1.4 Protección contra amenazas externas y ambientales

AdC, debe proveer las condiciones físicas y medio ambientales necesarias para brindar la protección de las personas y la seguridad de la información de la Entidad, ante posibles eventos como incendios, inundaciones, terremotos, explosiones, ataques maliciosos, entre otros. Por lo anterior se debe dar cumplimiento a los siguientes lineamientos:

a. La oficina de tecnología de la información, debe propender por la seguridad del (Datacenter y Centros de Cableado) que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

b. El propietario del activo de información debe propender porque la Información se almacene en un ambiente protegido y seguro.

10.7.1.5. A.11.1.5 Trabajo en áreas seguras

a. En el Datacenter y Centros de Cableado, deben existir sistemas de control ambiental de temperatura, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

b. La oficina de tecnologías de la información, debe velar porque los recursos de la plataforma tecnológica de la Entidad, estén ubicados en el Datacenter (Interno o Externo) con protecciones contra fallas o interrupciones eléctricas.

c. La oficina de tecnologías de la información, debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo, autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos. Durante la actividad este personal debe estar acompañado de manera permanente por personal autorizado de la entidad.

d. La oficina de tecnologías de la información, debe tener control de: (cualquier cambio, modificación, actualización, ajuste o soporte) que se realice sobre los procesos, áreas seguras y sistemas de procesamiento de información, que puedan afectar uno o más de los “Pilares de Seguridad de Información (Confidencialidad Integridad y Disponibilidad)”; para ello deben pasar por la aprobación del Comité de Cambios TI antes de su ejecución.

e. En las áreas seguras no está permitido el registro fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con una autorización del profesional o área encargada del área segura, para ello.

10.7.1.6 A.11.1.6 Áreas de Despacho y Carga

AdC define controles para restringir el acceso a personal no autorizado en áreas de carga y despacho:

- El área de carga y despacho deben estar claramente definida.
- En los casos que aplique la puerta de acceso al interior de la compañía desde el área de carga y descarga deben permanecer cerradas y con control de acceso restringido.
- Las puertas externas deben permanecer cerradas mientras se efectúa el cargue o despacho.
- El material que llega o sale, se debe registrar, revisar e inspeccionar que sea el que corresponde con la lista de verificación, y que no contenga materiales o líquidos extraños que pueda ocasionar daños o afectar la seguridad de la información.
- Se debe restringir los accesos al área de carga y descarga desde fuera de las instalaciones y solamente al personal autorizado y debidamente identificado.
- Las áreas de entrega de reciclaje deben ser monitoreadas y custodiadas por personal de vigilancia mientras se realiza la entrega.

10.7.2 A.11.2 EQUIPOS

Dominio/ Control: A.11.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros que tengan acceso a la información, en medio digital o físico, de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.7.2.1 A.11.1.2 Ubicación y protección de equipos

a. Los computadores portátiles y de escritorio tipo "todo en uno" asignados a los servidores públicos, contratistas, pasantes, proveedores y terceros de la entidad, deben estar ubicados en áreas donde se reduzca el riesgo de pérdida o robo.
b. Los equipos que tienen o manejan información sensible o confidencial, deben estar ubicados en áreas donde el acceso es restringido.
c. Los sistemas de información y los equipos de comunicaciones que requieren protección especial deben estar aislados para reducir el nivel del riesgo al que puedan estar expuestos.
d. Las condiciones ambientales en las instalaciones donde se encuentran los servidores y equipos activos (switches, enrutadores, entre otros), deben ser adecuados, deben contar aire acondicionado, detector de humo, puerta antipánico.
e. Está prohibido el consumo de bebidas y comidas en las instalaciones de procesamiento de información.
f. Está prohibido fumar dentro de las instalaciones de AdC.
g. Las impresoras, fotocopiadoras, escáneres y/o multifuncionales que procesan información confidencial deben ser ubicadas en áreas seguras para prevenir el acceso, transmisión no autorizada o duplicación de documentos.
h. Para prevenir y minimizar riesgos, la oficina de tecnologías de la información, debe establecer medidas de protección lógica que limitan el acceso de los usuarios a cada impresora o periférico compartido a través de la red de AdC.

10.7.2.2 A.11.2.2 Servicio de Suministro

a. La infraestructura tecnológica de la entidad, debe estar protegido contra problemas eléctricos que puedan causar una falla o mal funcionamiento de los mismos.
b. Los servicios de suministro como, electricidad, agua, alcantarillado, aire acondicionado, ventilación/calefacción se deben inspeccionar regularmente para garantizar su buen funcionamiento.

c. Frente a posibles fallas en el suministro de energía para los equipos en la compañía especialmente todos aquellos que sustentan las operaciones críticas para la continuidad de las actividades, se deben proveer sistemas de suministro eléctrico apoyado de fuentes de energía ininterrumpible como UPS.
d. Los equipos (computadores) deben estar conectados a las tomas de corriente regulada.
e. Se debe monitorear periódicamente el funcionamiento de los equipos de soporte, verificando que cumplan con requisitos de configuración y capacidad recomendados por el fabricante (por ejemplo: U.P.S., aire acondicionado, planta eléctrica, entre otros).

10.7.2.3 A.11.2.3 Seguridad de cableado

a. La dependencia encargada de la gestión de recursos físicos, debe garantizar que dentro de la infraestructura física de AdC, el cableado de energía eléctrica y de telecomunicaciones que transporta los datos o soporta los Servicios de Información de la entidad, deben estar protegidos para evitar daño o mala manipulación.

b. Las áreas de distribución de redes deben estar físicamente aseguradas para prevenir la modificación o el acceso no autorizado a las mismas.

10.7.2.4 A.11.2.4 Mantenimiento de equipos

a. La instalación de cualquier tipo de software en los equipos de la entidad, es responsabilidad de la oficina de tecnologías de la Información y por tanto son los únicos autorizados para realizar y/o autorizar esta labor, que se realizará con usuario administrador del equipo local.

b. El mantenimiento de los equipos, se deben realizar a intervalos planificados teniendo en cuenta las especificaciones y recomendaciones de los fabricantes; por lo que es necesario llevar un registro de las fallas presentadas.

c. La Mesa de ayuda de la Entidad, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración) a equipos personales.

d. Los usuarios no deben realizar cambios en los equipos de la Entidad; referente a: la configuración del equipo, conexiones de red, papel tapiz y protector de pantalla definido por AdC, fotografía personal en el usuario de correo institucional. Estos cambios pueden ser realizados únicamente por el personal de la Mesa de Ayuda designado para tal labor por parte de la oficina de tecnologías de la información, a través de una solicitud de ticket previamente autorizada.

10.7.2.5 A.11.2.5. Retiro de activos

a. El retiro de equipos de la entidad, deberá estar justificado y autorizado por el jefe de área donde está ubicado el equipo, y visto bueno de la oficina de tecnologías de la información y/o el Oficial de Seguridad de Información.
b. El retiro de equipos y/o software de la entidad, deberá estar justificado y autorizado por el jefe de área donde trabaja el usuario.
c. No obstante, mientras el activo se encuentre en poder del usuario, cada vez que ingrese o salga de las instalaciones de la compañía, en cada portería debe ser registrado en la planilla destinada para este fin.
d. Los tiempos de retiro se definen de acuerdo con la actividad a realizar.
e. El recibo y entrega de los equipos se debe formalizar a través del formato establecido por la entidad. En caso del cese de labores del usuario, éste debe entregar los elementos proporcionados por la entidad a través del formato de paz y salvo definido por la entidad.

10.7.2.6 A.11.2.6 Seguridad de equipos y activos fuera de las Instalaciones

a. Se deben asegurar los equipos de la entidad, fuera de las instalaciones y su salida debe estar autorizada por el responsable del área a la cual esté asignada la máquina.
b. Las personas que son autorizadas para retirar cualquier equipo de las instalaciones de AdC, son los responsables directos de su protección.
c. Para el uso de los equipos fuera de las instalaciones se debe tener en cuenta las consideraciones del Instructivo Clasificación y rotulado de la información y el instructivo de Uso aceptable de los activos.

10.7.2.7 A.11.2.7 Disposición segura o reutilización de equipos

a. Toda la información de la entidad, tendrá que ser removida del equipo antes de su disposición o reutilización, previa generación de backup de la información allí almacenada.

b. Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación o borrado seguro de información que adopte la entidad, previa generación de backup de la información allí almacenada.

10.7.2.8 A.11.2.8 Equipos de usuarios desatendidos

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección y están obligados a:

a. No dejar la sesión abierta, cuando se ausente del puesto de trabajo.
b. En el momento de dejar desatendido el computador o portátil en el puerto de trabajo, el usuario debe bloquear su equipo usando las teclas: “Botón de windows + la tecla L” o “Ctrl + ALT+ SUPR + ENTER”.
c. Bloquee la sesión y/o cierre la sesión de usuario, cuando finalice la tarea (no es correcto apagar la pantalla o el equipo sin salir de la sesión de usuario).
d. Los equipos que se encuentren bloqueados deberán contar con protector de pantalla definido por la entidad, de acuerdo al tiempo límite de inactividad definido por el Administrador.

10.7.2.9 A.11.2.9 Política de escritorio y pantalla limpios

a. Escritorio limpio

La política de escritorio limpio aplica para todos los equipos de propiedad de la entidad por lo que se debe dar cumplimiento de los siguientes lineamientos:

- Proteja la información siempre que abandone su puesto de trabajo.
- No se deben dejar documentos con información Sensible o Confidencial, al alcance de personal no autorizado, en caso de tener este tipo de información en físico ésta debe ser guardada bajo llave en archivadores.
- No se debe dejar documento que se encuentre en tránsito al alcance de personal no autorizado, independiente de su clasificación que contiene información institucional.
- No se debe consumir líquidos en el puesto de trabajo.

b. Pantalla Limpia

- El escritorio virtual del equipo de cómputo debe permanecer libre de documentos digitales, independiente de su clasificación de información.

10.8 A.12 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

Dominio/ Control: A.12 Seguridad en las Operaciones.

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Alcance: La presente Política aplica para todas las operaciones que se desarrollen en la Entidad, a través de servidores públicos, contratistas, pasantes, proveedores y terceros, con los que interactúa AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.8.1 A.12.1 PROCEDIMIENTOS DE OPERACIONES Y RESPONSABLES

10.8.1.1 A.12.1.1 Procedimientos de operación documentado

a. Los procedimientos operativos se deben documentar y poner a disposición de los servidores públicos, contratistas, pasantes, proveedores y terceros que los necesitan para la ejecución de sus funciones.

b. Los procedimientos operativos específicos de la Entidad, deben ser tratados como documentos formales y los cambios que se generen deben ser autorizados.

c. Se debe mantener un diagrama actualizado de la red de la Entidad.

d. La oficina de tecnologías de la información, debe mantener una lista documentada y actualizada de los Servicios, Protocolos y Puertos Utilizados, incluyendo la justificación pertinente en los casos que se estén utilizando protocolos no seguros. En el caso de detectar protocolos inseguros, se debe contar con contramedidas para cerrar las vulnerabilidades encontradas.

10.8.1.2 A.12.1.2 Gestión de cambios

a. La oficina de tecnologías de la información, debe implementar un proceso documentado para la Gestión de Cambios, que aplique para todos los procesos relacionados con la gestión de TI en cuanto a las instalaciones, los sistemas de información e infraestructura, donde se pueda ver comprometida la seguridad de la información.

b. Solo se deben habilitar los Servicios y Protocolos necesarios y seguros según lo requiera la función del Sistema solicitado.

10.8.1.3 A.12.1.3 Gestión de capacidad

La oficina de tecnologías de la información, debe realizar un análisis de capacidades y proyecciones para el procesamiento y almacenamiento disponible de la información. Estas proyecciones deben tener en cuenta:

- Los nuevos requerimientos de Sistemas de Información de los Procesos.
- Cambios tecnológicos.
- El crecimiento de los Sistemas actuales de Procesamiento de la Información.

10.8.2 A.12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Dominio: A.12.2. Protección contra códigos maliciosos.

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.8.2.1 A.12.2.1 Controles contra código malicioso

a. La oficina de tecnologías de la información, debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de AdC y los servicios que se ejecutan en la misma.

b. La oficina de tecnologías de la información debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y derechos de actualizaciones, para mitigar las vulnerabilidades de la plataforma tecnológica

c. La oficina de tecnologías de la información debe garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.

d. La oficina de tecnologías de la información, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

e. La Oficina de tecnologías de la información debe asegurar que, al momento de conectarse un dispositivo de almacenamiento externo, se ejecute el software de antivirus de manera automática.

f. Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos, descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas para evitar el contagio de virus informáticos, ejecución o instalación de programas con software malicioso en los recursos tecnológicos.

g. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de ayuda para que se tomen las medidas de control correspondientes.

10.8.3 A.12.3 COPIAS DE RESPALDO

10.8.3.1 A.12.3.1 Respaldo de la información

a. La oficina de tecnologías de la Información, debe definir un procedimiento para las actividades de backup de la Información de la Entidad, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para seguimiento y control.

b. Es responsabilidad de quien(es) ejecute(n) el rol de administrador de cada Sistema de información, realizar la solicitud de copia a quien(es) ejecute(n) el rol de administrador de backup, validar y asegurar que su Sistema de Información se encuentre contemplado en el cronograma de copias de seguridad, además de hacer seguimientos regulares a su ejecución.

c. Quien (es) ejecute (n) el rol de Administrador de backup debe validar el resultado de la ejecución de las copias de Seguridad y registrar las novedades en la bitácora establecida para ello como lo debe indicar el procedimiento.

d. Es responsabilidad de quien (es) ejecute (n) el rol de Administrador de backup realizar pruebas de restauración de copias de seguridad de manera trimestral siguiendo los lineamientos del Procedimiento Backup y Recuperación de la Información.

e. Cada copia de seguridad debe quedar registrada en la máquina donde son realizados (logs de servidor) o en un archivo externo (texto, planilla, etc.) que permita mantenerla disponible para controles o auditoría.

f. En lo posible los medios de respaldo removibles deben ser trasladados a un lugar externo que garantice el catálogo, la fiabilidad, seguridad y disponibilidad de estos. Para ello se debe asegurar un transporte o un servicio de mensajería fiable que cuente con todas las medidas de seguridad.

10.8.4 A.12.4 REGISTRO Y SEGUIMIENTO

10.8.4.1 A.12.4.1 Registro de eventos

a. Se deben generar y mantener registros de auditoría sobre las actividades de los usuarios, excepciones y eventos de seguridad de información para soportar futuras investigaciones y monitoreo del control de acceso.

10.8.4.2 A.12.4.2 Protección de la información de registros

a. Los registros de información se deben proteger contra intentos de alteración y acceso no autorizado.

10.8.4.3 A.12.4.3 Registros de Administrador de Operador

a. Todas las evidencias que se recolectan como resultado de las auditorías practicadas, deben contar con un lugar para el almacenamiento de los registros y monitoreo de los eventos de seguridad.

b. Todo acceso administrativo a sistemas críticos de la Entidad que no sea por consola debe ser accedido de forma segura (protocolos SSH, HTTPS).

10.8.4.4 A.12.4.4 Sincronización de relojes

a. Se debe tener como referencia la hora legal colombiana y no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora. Los relojes de todos los sistemas de procesamiento de información relevantes dentro de AdC deben estar sincronizados con la fuente oficial.

b. El ajuste correcto de los relojes de computador es importante para asegurar la exactitud de los registros de auditoría (Logs), que pueden ser necesarios para investigaciones o como evidencia legal o en casos disciplinarios.

10.8.5 A.12.5 CONTROL DE SOFTWARE OPERACIONAL

10.8.5.1 A.12.5.1 Instalación de software en sistemas operativos

a. La oficina de tecnologías de la información, debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, de acuerdo con los procedimientos establecidos para ello.
b. La oficina de tecnologías de la información, debe asegurarse que el software operativo instalado en la plataforma tecnológica cuente con soporte de los proveedores.
c. La oficina de tecnologías de la información, debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
d. La oficina de tecnologías de la información debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
e. La oficina de tecnologías de la información debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la entidad.

10.8.6 A.12.6 GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

10.8.6.1 A.12.6.1 Gestión de las Vulnerabilidades Técnicas

a. La oficina de tecnologías de la información, debe implementar procedimientos para la gestión de vulnerabilidades técnicas y remediación de las mismas.
b. La ejecución del análisis de vulnerabilidades tiene como fin, identificar las brechas de seguridad con las que cuenta un sistema de información y la infraestructura

tecnológica, por lo tanto, la Entidad debe ejecutar análisis de vulnerabilidades a los activos de información. Se deben:

- Documentar los resultados.
- Priorizar las vulnerabilidades.
- Documentar el plan de remediación para corregir o mitigar (según sea el caso) las brechas identificadas.
- Entregar los resultados de las pruebas realizadas a cada uno de los responsables de los sistemas de información e infraestructura tecnológica, quienes son los encargados de definir y aplicar el plan de remediación.

c. La oficina de tecnologías de la información, debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica con el fin de prevenir la exposición al riesgo de estos.
d. La oficina de tecnologías de la información a través de sus empleados, debe generar, ejecutar y hacer seguimiento a los planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
e. Dependiendo de la prioridad con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debe a llevar a cabo de acuerdo con los procedimientos de Gestión de cambios y/o Gestión de incidentes de seguridad de la información.

10.8.7 A.12.7 CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

10.8.7.1 A.12.7.1 Controles de Auditoria de Sistemas de Información

a. Las auditorías que involucran accesos a los sistemas de información deben ser planificadas y acordadas, para minimizar las interrupciones en los procesos del negocio.
b. Las auditorías deben estar orientadas a evaluar aspectos técnicos de seguridad de la información que apoyan la operación del negocio.
c. Las pruebas de auditoría deben desarrollarse en ambientes que no afecten la operación del negocio.

10.9 A.13 POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

Dominio/ Control: A.13 Seguridad de las Comunicaciones

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de AdC.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.9.1 A.13.1 GESTIÓN DE LA SEGURIDAD LAS REDES

10.9.1.1 A.13.1.1 Controles de Redes

a. Se deben controlar los accesos a servicios internos y externos conectados en red.

b. Los servidores públicos, contratistas, pasantes, proveedores y terceros, antes de contar con acceso lógico por primera vez a la red de datos de AdC, deben contar con la autorización previa por parte de su Jefe inmediato y/o supervisor del Contrato, para proceder a la creación, activación de las cuentas de usuario, está solicitud se debe hacer a la oficina de tecnologías de la información por el canal definido por la Entidad.

c. Los servidores públicos, contratistas, pasantes, proveedores y terceros, antes de contar con acceso lógico por primera vez a la red de datos de AdC, deben contar con la autorización respectiva como lo indica el procedimiento establecido para ello.

d. El acceso a los sistemas de la red se debe hacer a través de usuarios autorizados.

e. Los sistemas deben permitir llevar un registro y seguimiento para detectar acciones que puedan afectar la seguridad de la información.

10.9.1.2 A.13.1.2 Seguridad de los servicios de red

a. La oficina de tecnologías de la información de la Entidad, como responsable de las redes de datos y los recursos de red de AdC (internos y externos), debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

b. En los acuerdos con proveedores se deben identificar e incluir acuerdos de niveles de Servicio ANS) como mecanismos de seguridad, al igual que el derecho de poder hacer seguimiento con regularidad y acordar el derecho de auditoría

10.9.1.3 A.13.1.3 Separación en las Redes

a. La oficina de tecnologías de la información, debe implementar mecanismos de control a través de segmentación de las redes en función de los grupos de servicios.
b. La oficina de tecnologías de la información, debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica con el fin de reducir el acceso no autorizado y evitar cambios inadecuados sobre los servicios de T.I. (servicios de red, acceso a sistemas de información, servicios de internet).
c. La oficina de tecnologías de la información, debe asegurar que las redes inalámbricas de AdC, cuenten con procedimientos de autenticación para evitar accesos no autorizados a servidores públicos, contratistas, pasantes, proveedores y terceros.

10.9.2 A.13.2 TRANSFERENCIA DE INFORMACIÓN

Dominio/Control: A13.2 Transferencia de Información.

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Alcance: La presente política aplica para servidores públicos, contratistas, pasantes, proveedores y terceros que por su rol, transfieran información dentro de la entidad y con cualquier entidad externa.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.9.2.1 A.13.2.1 Políticas y procesamiento de transferencia de información

a. La entidad establece los mecanismos de control formales para proteger la transferencia de información, a través de los servicios soportados en su infraestructura tecnológica.

10.9.2.2 A.13.2.2 Acuerdos sobre transferencia de información

a. Cuando se trate de intercambios periódicos, se debe privilegiar la transmisión de datos a través de vías seguras, con los cuales se establecen convenios o nexos de diferente naturaleza, y que involucran de alguna forma el intercambio de información.

b. Para el acceso a sitios web, se debe implementar herramientas de seguridad perimetral seguros (firewalls) y el uso de protocolos seguros.

10.9.2.3 A.13.2.3 Mensajería Electrónica

a. Todos los mensajes enviados desde la cuenta Institucional de la entidad, deben respetar el estándar de formato e imagen Corporativa de AdC.

b. La transmisión de archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable serán bloqueados, en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la oficina de tecnologías de la información.

c. El uso del correo electrónico en cadenas o mensajes enviados a un número de destinatarios y estos a su vez son enviados a otros, sin un propósito relacionado con la misión de AdC, degradan el desempeño del Servicio de Correo y consumen recursos de TI valiosos. El usuario debe abstenerse de enviarlos a otras personas.

d. No enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos. Si un usuario encuentra este tipo de material deberá reportarlo a la mesa de ayuda.

e. La Entidad, debe asignar una cuenta de correo electrónico como herramienta de trabajo para cada uno de los servidores públicos, contratistas y pasantes o quien por su rol, lo requieran para el desempeño de sus Funciones y/o Obligaciones y en algunos casos a terceros previa autorización; su uso se encuentra sujeto a lo establecido en la presente Política.

f. Los mensajes y la información contenida en los buzones de correo son de propiedad de AdC, y cada usuario es responsable de su buzón, por lo que debe mantener solamente los mensajes relacionados con el desarrollo de sus Funciones y /o Obligaciones.

g. El correo electrónico, deberá tener al final del mensaje el siguiente texto:

Este mensaje y cualquier archivo anexo podrían contener información confidencial, clasificada o reservada de uso uso exclusivo de su destinatario. La utilización, copia, reimpresión y/o reenvío del mismo por personas distintas al destinatario están expresamente prohibidos. Si usted no es destinatario, favor notificar en forma inmediata al remitente y borrar el mensaje original y cualquier archivo anexo.

10.9.2.4 A.13.2.4 Acuerdos de confidencialidad o de no divulgación

a. La presente política de confidencialidad, tiene por objeto informarles a todos los servidores públicos, contratistas, pasantes, proveedores y terceros o quien por su rol estén vinculados con AdC, sobre el compromiso frente a la no divulgación de la información relacionada con las funciones y/o obligaciones contractuales que desempeña en la Entidad, a personal interno o externo de la misma.

b. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros o quien por su rol estén vinculados con AdC, deben firmar la cláusula y/o acuerdos de confidencialidad definidos, y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.

c. AdC, firmará acuerdos de Confidencialidad con los Clientes y Terceros o Contratistas, que por diferentes razones requieran conocer o intercambiar información Reservada o Confidencial de la Entidad. En estos los acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

d. El acuerdo de Confidencialidad deberá formalizarse en cada uno de los contratos celebrados con Terceros y que en la Prestación del Servicio puedan tener acceso a la información Reservada o Confidencial de la Entidad.

e. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros de AdC, deben guardar absoluta reserva en relación con la información a la que tenga acceso con ocasión de la ejecución del Funciones y/o Obligaciones, aún después de finalizada su ejecución, por el tiempo establecido por la normatividad legal vigente y aplicable para cada caso en particular.

10.10 A.14 POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Dominio/ Control: A.14.1 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

AdC a través de la oficina de tecnologías de la información y el oficial de seguridad de la información, asegurará que el software adquirido cumpla con los requisitos de seguridad y calidad establecidos por la entidad.

10.10.1 A.14.1. REQUISITOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

10.10.1.1 A.14.1.1 Análisis y especificaciones de requerimientos de seguridad de la información

a. Los propietarios de los sistemas de información de la Entidad, deberán identificar y documentar qué tipo de clasificación de la información se encuentra contenida en los mismos.

b. Los propietarios de los Activos de Información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información definida por la Entidad.

c. Para la adquisición y actualización de software se requiere la participación y compromiso del funcionario del área quien define los requerimientos funcionales y con el apoyo de la oficina de tecnologías de la información define los aspectos tecnológicos y de requerimientos no funcionales, que deberán ser parte de la evaluación y aprobación de las propuestas presentadas.

d. La adquisición, desarrollo y mantenimiento de sistemas de información incluye buenas prácticas de seguridad digital durante todo el ciclo de vida, los requisitos relacionados con la seguridad digital son incorporados a los sistemas de información tanto nuevos como ya existentes. Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.

e. Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.

f. Se debe garantizar que el software adquirido cuente con los contratos de mantenimiento y actualizaciones respectivas.

10.10.1.2 A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

En lo que respecta a la autorización y continuidad de los usuarios de los sistemas de información y/o aplicativos de AdC, será deber de cada uno de los responsables de los procesos o proyectos de la entidad, informar a los administradores de las aplicaciones la novedad o novedades que surjan de los servidores públicos, contratistas, pasantes, proveedores y terceros, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuese el caso.

10.10.1.3 A.14.1.3 Protección de Transacciones de los Servicios de las Aplicaciones

a. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

b. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) establecer los controles de acceso a los ambientes de producción de los sistemas de información.

c. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

d. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que en lo que respecta a los sistemas operativos de la entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.

e. Quien (es) ejecute (n) el rol de desarrollador de sistemas de información debe (n) garantizar que se cierre la sesión en las aplicaciones, después de determinados minutos de inactividad (Timeout) previamente establecidos.

f. Se debe asignar el rol del Administrador de programas fuentes, quien tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no deberá pertenecer al equipo de desarrollo.

g. La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización de acuerdo con los lineamientos definidos de la oficina de Tecnologías

h. Se debe aplicar un procedimiento que garantice que en toda migración a producción el módulo fuente genera el código ejecutable correspondiente en forma automática.

i. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe(n) asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

j. No está permitido facilitar el usuario o la contraseña a otra persona para adelantar cualquier labor en los Sistemas de Información y Aplicaciones.

10.10.2 A.14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

Dominio/ Control: A.14.2 Seguridad de los Procesos de Desarrollo Seguro.

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información

Alcance: La presente política aplica a los Sistemas de Información, sean desarrollos internos o de terceros.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

a. Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

b. Se debe implementar el Procedimiento de Control de Cambios definidos por la Entidad, cuando se realicen cambios a los Sistemas de Información; este cambio puede ser:

- Modificación a Sistemas de Información en Producción (campos, tablas, parámetros, entre otros).
- Nuevos Requerimientos a Sistemas de Información en Producción (módulos, tablas, campos, entre otros).
- Nuevos Sistemas de Información (desarrollo in house o externo).
- Cambios reglamentarios.
- Y demás que afecten los Sistemas de Información por necesidades puntuales de la Entidad.

c. Realizar las pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos en ambientes de pruebas y producción, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción, considerando nuevos sistemas, nuevas funcionalidades, mantenimientos en aplicaciones construidas internamente, construidas por proveedores, aprovisionadas en la nube o híbrido de las anteriores.

d. Generar, adoptar o recomendar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

e. Aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos, cambios, o nuevas funcionalidades.

10.11 A.15 RELACIÓN CON LOS PROVEEDORES

Dominio/ Control: A.15 Relación con los Proveedores.

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores

Alcance: La presente Política aplica para todos los Proveedores o Terceros, que requieran acceso a los Activos de Información de la Entidad.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.11.1 A.15.1 SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES

10.11.1.1 A.15.1.1 Política de Seguridad de Información para las Relaciones con Proveedores

a. La Entidad, durante la Etapa Precontractual, desde la construcción de los estudios previos, el Área solicitante de la contratación, debe identificar los Riesgos de Seguridad de la Información con el apoyo del Líder u Oficial de Seguridad de la Información, los cuales deben ser parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

b. La Entidad, en cabezada del Comité evaluador debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a:

- A la información Reservada o Confidencial.
- A los Sistemas de Información.
- A las Áreas Seguras.

c. El Comité evaluador debe contar con la participación del Líder u oficial de seguridad de la información a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato.

d. En medio de la Etapa Contractual, se debe asegurar la inclusión de las cláusulas:

- De Confidencialidad.
- De Protección de Datos.
- Derechos de Propiedad Intelectual.
- Las Políticas de Seguridad y Privacidad de la Información definida por la Entidad.

- Derechos de Autor.

10.11.1.2 A.15.1.2 Tratamiento de Seguridad dentro de los Acuerdos con Proveedores

a. Antes de iniciar la ejecución del contrato, el supervisor debe socializar a los Proveedores:

- Las Políticas de Seguridad y Privacidad de la Información.
- Los procedimientos asociados al Sistema de Gestión de Seguridad de la Información.

b. Durante la Etapa Post Contractual, es función del supervisor y/o interventoría asignada, monitorear y hacer seguimiento a los controles pactados para asegurar la Confidencialidad, Integridad y Disponibilidad de la Información, frente a los riesgos previamente identificados.

10.11.1.3 A.15.1.3 Cadena de Suministro de Tecnología de Información y Comunicaciones

a. Para los Servicios de Tecnología y de Comunicaciones contratados externamente, se debe exigir que los Proveedores divulguen los requisitos y prácticas de Seguridad de AdC, a lo largo de la cadena de suministro.

b. Para la contratación de servicios o componentes de la Infraestructura de TI y/o Áreas Seguras, se debe exigir a los Proveedores la presentación de los Planes de Contingencia que aseguren la Disponibilidad de la Información, suministrada y procesada entre las partes.

10.11.2 A.15.2 GESTIÓN DE PRESTACIÓN DE SERVICIO DE PROVEEDORES

10.11.2.1 A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

a. Como parte de la supervisión a la ejecución del contrato, se debe contemplar procesos de auditoría a proveedores cuyo objetivo sea validar el cumplimiento de los requisitos de Seguridad de la Información estipulados en la etapa contractual, dichos resultados deben quedar consignados también en los informes presentados por el supervisor del contrato.

10.11.2.2 A.15.2.2 Gestión de Cambios en los Servicios de los Proveedores

a. Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al Servicio de Tecnología de la Información, Comunicaciones o Equipos de Suministros, debe pasar por el Procedimiento Gestión de Cambios y seguir las directrices del Líder u Oficial de Seguridad de la Información, antes de su ejecución.

10.12 A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Dominio/ Control: A.16 Gestión de Incidentes de Seguridad de la Información.

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

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros, los cuales deben reportar todo Evento o Incidente de Seguridad de la Información a la mesa de ayuda, a través de los canales oficiales establecidos por la Entidad, y estos a su vez, deben ser gestionados por los responsables de acuerdo con el procedimiento establecido para tal fin.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.12.1 A.16.1 GESTIÓN DE INCIDENTES Y MEJORA EN LA SEGURIDAD DE LA INFORMACIÓN

10.12.1.1 A.16.1.1 Responsabilidades y Procedimientos

a. AdC promoverá entre los servidores públicos, contratistas, pasantes, proveedores y terceros el deber de reportar los incidentes relacionados con la seguridad de la información.

b. Los propietarios de los Activos de Información, deben informar a la oficina de tecnología de la información de AdC, a través de la mesa de ayuda los Eventos e Incidentes de Seguridad que identifiquen o que reconozcan ante su posibilidad de materialización.

c. AdC en cabeza del Oficial de Seguridad gestionará el incidente de seguridad y se apoyará con las áreas afectadas para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigarlo y solucionarlo, tomando las medidas necesarias para evitar su reincidencia.

d. Para la gestión de los incidentes de seguridad de la información, se deben seguir los lineamientos del procedimiento Gestión de incidentes y el formato Incidentes de seguridad de la información definidos por la entidad.

10.12.1.2 A.16.1.2 Reporte de Eventos de Seguridad de Información

a. Todos los servidores públicos, contratistas, pasantes, proveedores y terceros de AdC, que tengan acceso a información sensible, confidencial e interna, a través de:

- Infraestructura tecnológica (software, hardware y servicios tecnológicos).
- La información física.
- Las personas.
- Demás medios en el que se encuentre información de la Entidad.

b. Deben reportar de manera oportuna y a través de los medios establecidos por la entidad, los eventos de seguridad de la información técnicos y no técnicos, donde se puedan ver comprometidos la confidencialidad, disponibilidad e integridad de los activos de información. Lo anterior siguiendo los lineamientos del procedimiento Gestión de incidentes.

10.12.1.3 A.16.1.3 Reporte de Debilidades de Seguridad de Información

a. Los servidores públicos, contratistas, pasantes, proveedores y terceros de AdC, que hagan uso de la infraestructura tecnológica de la entidad, deben informar a través de los canales oficiales establecidos por la empresa y de acuerdo con el procedimiento Gestión de incidentes, aquellas debilidades que puedan comprometer los activos de información.

b. El incumplimiento al uso adecuado de los activos de información de AdC por los servidores públicos, contratistas, pasantes, proveedores y terceros, podría ser interpretado como un mal uso potencial derivando en la respectiva investigación y sanciones según el caso.

10.12.1.4 A.16.1.4 Evaluación de los Eventos de Seguridad de la Información y Decisiones Sobre Ellos

a. Los Incidentes deben ser atendidos a través de una serie de normas, reglamentos, procedimientos y/o protocolos a seguir, donde se definen las distintas medidas a tomar para identificar, prevenir, priorizar los Incidentes identificados los cuales se les debe documentar, solucionar, realizar seguimiento y posterior cierre por las responsables del equipo de manejo de Incidentes al interior de AdC o Entidades externas según sea el caso; al igual se debe tener en cuenta los aspectos Legales a los cuales se debe dar cumplimiento.

b. AdC en cabeza del Oficial de Seguridad analizará si el evento de seguridad de la informatización reportado corresponde a un incidente de seguridad de la información para su gestión, de acuerdo con el procedimiento Gestión de incidentes.

c. AdC deberá consolidar una base de datos de conocimiento que podrá ser utilizada como apoyo para gestionar incidencias de seguridad relacionados.

10.12.1.5 A.16.1.5 Respuesta a Incidentes de Seguridad de la Información

a. AdC, debe designar personal calificado, para gestionar adecuadamente los incidentes de seguridad de la información reportados, siguiendo los lineamientos del procedimiento Gestión de incidentes, para garantizar la seguridad y la continuidad del servicio comprometidos.

10.12.1.6 A.16.1.6 Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

a. Las lecciones aprendidas a través de los incidentes de seguridad de la información deben ser socializadas con todos los servidores públicos, contratistas, pasantes, proveedores y terceros según corresponda, como ejemplos de lo que podría ocurrir, cómo responder a estos incidentes y cómo evitarlos en el futuro.

10.12.1.7 A.16.1.7 Recolección de Evidencia

a. AdC incluye en el procedimiento Gestión de incidentes actividades para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia con propósitos de acciones legales y/o disciplinarias.

- La identificación, es el proceso que involucra la búsqueda, reconocimiento y documentación de evidencia potencial.
- Recolección, es el proceso de reunir elementos físicos que pueden contener evidencia potencial.
- Adquisición, es el proceso de crear una copia de los datos dentro de un grupo definido.
- Preservación, es el proceso de mantener y salvaguardar la integridad y la condición original de la evidencia potencial.

b. AdC se asegura que la identificación, recolección, adquisición y preservación de evidencias, sea realizado por personal idóneo donde se cumpla con las siguientes características:

- La cadena de custodia;
- La seguridad de la evidencia;
- La seguridad del personal;
- Los roles y responsabilidades del personal involucrado;
- La competencia del personal;
- La documentación;
- Las sesiones informativas

Si no se cuenta con las capacidades (conocimiento, herramientas y demás), esta actividad deberá ser contratada externamente o apoyada con las autoridades competentes.

10.13 A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Dominio/ Control: A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.

Objetivo: La Continuidad de Seguridad de la Información se debería incluir en los Sistemas de Gestión de la Continuidad de Negocio de la organización.

Alcance: La presente Política establece que AdC, debe determinar sus requisitos para la Continuidad del Negocio, basados en la planificación, implementación y verificación de los mismos, para todos los procesos de la Entidad.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.13.1 A.17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

10.13.1.1 A.17.1.1 Planificación de la Continuidad de la Seguridad de la Información

a. AdC, debe determinar sus requisitos para la Seguridad de la Información y la Continuidad de la Gestión de la Información en situaciones adversas durante una crisis o desastres.

b. AdC a través de la oficina de planeación e información; debe liderar el Plan de Continuidad del Negocio.

c. AdC, debe establecer, documentar y mantener procesos, procedimientos para asegurar el nivel de Continuidad requerido para la Seguridad de la Información durante una situación adversa.

10.13.1.2 A.17.1.2 Implementación de la Continuidad de la Seguridad de la Información

a. La oficina de tecnologías de la información, debe elaborar el Plan de Recuperación Ante Desastres (DRP) y retorno a la normalidad, para cada uno de los Servicios y Sistemas de Información que tengan un impacto alto en los Procesos de AdC.
b. AdC debe establecer, documentar, aprobar, implementar y mantener planes, procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
c. AdC, debe contar con una estructura de gestión adecuada para prepararse, mitigar y responder ante un evento perturbador usando personal con la autoridad, experiencia y competencias.

10.13.1.3 A.17.1.3 Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información

a. AdC, debe asegurar la realización de pruebas periódicas del Plan de Recuperación Ante Desastres (DRP) y/o Continuidad de Negocio, verificando la Seguridad de la Información durante su realización y la documentación de dichas pruebas.

b. AdC, debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

10.13.2 A.17.2 REDUNDANCIA

10.13.2.1 A.17.2.1 Disponibilidad de las Instalaciones de Procesamiento de Información

a. La oficina de tecnologías de la información, debe asegurar de acuerdo con sus capacidades la disponibilidad de instalaciones de Procesamiento de Información de AdC y propender por la existencia de una Plataforma Tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Entidad.

b. La oficina de tecnologías de la información, debe analizar y establecer los requerimientos de redundancia para los Sistemas de Información esenciales para la Entidad y la Plataforma Tecnológica que los apoya.

c. La oficina de tecnologías de la información, debe evaluar y probar soluciones de redundancia Tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Entidad.

d. La oficina de tecnologías de la información, a través de sus colaboradores como: servidores públicos, contratistas, pasantes, proveedores y terceros, los cuales deben administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Entidad.

10.14 A.18 CUMPLIMIENTO

Dominio/ Control: A.18 Cumplimiento.

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información y de cualquier requisito de Seguridad.

Alcance: La presente Política establece que se debe dar cumplimiento a los requisitos estatutarios, reglamentarios y contractuales pertinentes, establecidos por la Entidad a través de las Políticas de Seguridad y Privacidad de la Información.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

10.14.1 A.18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

10.14.1.1 A.18.1.1 Identificación de la Legislación Aplicable y de los Requisitos Contractuales

a. La Entidad, identifica los requisitos estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información, formalizados a través de su normograma.

10.14.1.2 A.18.1.2 Derecho de Propiedad Intelectual

a. La entidad implementará las medidas a que haya lugar para asegurar el cumplimiento de ley y requerimientos regulatorios y contractuales acerca de la propiedad intelectual (derechos de autor, patentes, entre otros) y el uso de productos de software.

- Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor.
- Crear conciencia sobre los derechos de propiedad intelectual.
- La oficina de tecnologías de la información, debe garantizar que solo haya instalado software autorizado y productos con licencia.
- Está prohibido reproducir total o parcialmente libros, artículos, reportajes, música, software u otros documentos diferentes de los permitidos por la ley de derechos de autor.

- La oficina de tecnologías de la información, debe establecer la línea base de software autorizado para ser instalado en las estaciones de trabajo.

10.14.1.3 A.18.1.3 Protección de Registros

a. La Entidad, deberá proteger los registros contra pérdida, destrucción, falsificación y acceso no autorizado; para dar cumplimiento a los Requisitos Legales.
b. Se debe garantizar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta su clasificación de acuerdo con el nivel de importancia.
c. Se deben definir los periodos de retención y conservación de la información. Los registros correspondientes a información confidencial o interna deben ser protegidos independientemente de los medios de conservación, ya sea física o digital. Los registros se deben clasificar por tipos de registros, por ejemplo, registros contables, registros de bases de datos, registros de transacciones (Logs), registros de auditoría (Audit Logs) y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos.
d. Cuando se escogen medios de almacenamiento electrónico, se deben establecer procedimientos para acceder a los datos (legibilidad de medios y de formatos) durante todo el período de retención, para proteger contra la pérdida debido a cambios futuros en la tecnología.
e. Se debe emitir directrices acerca de la retención, almacenamiento, manejo y disposición de registros e información, de acuerdo con los lineamientos del procedimiento establecido para ello.

10.14.1.4 A.18.1.4 Privacidad y Protección de Información de Datos Personales

Dominio: A.18.1.4 Privacidad y Protección de Información de Datos Personales.

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información, y de cualquier requisito de seguridad.

Alcance: La presente Política aplica para todos los servidores públicos, contratistas, pasantes, proveedores y terceros o que por su rol, tengan bajo su responsabilidad o suministren datos personales a la Entidad.

Lineamientos: Se debe dar cumplimiento de los siguientes lineamientos:

a. AdC en cumplimiento de lo establecido en la normatividad legal vigente aplicable a la privacidad y protección de datos personales en Colombia, actúa como Responsable de los datos personales que por virtud de sus funciones y competencias legalmente establecidas, le han sido suministradas y se encuentran en sus bases de datos siendo cada de una de las dependencias del Instituto él o la Encargado (a) del tratamiento.

b. Por tanto, AdC podrá dar tratamiento a los datos personales de TITULARES con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (civil, comercial y/o laboral, etc.) y entre los cuales se incluyen, pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas).

c. Salvo en los casos exceptuados por la ley, AdC solicitará a más tardar en la recolección de la información, autorización del TITULAR para capturar, almacenar, procesar, usar, circular, suprimir y en todo caso tratar los datos personales que hayan sido suministrados a la entidad por cualquier medio, bien sea digital o físico, y en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza; dicha autorización deberá estar contenida en un documento físico o electrónico.

d. Para todos los efectos, se entiende que la autorización por parte de los TITULARES a favor de AdC para el suministro y/o tratamiento de sus datos personales, realizada a través de los canales físicos o electrónicos, o por escrito o mediante conductas inequívocas, es:

- Expresa y voluntaria, lo que implica que EL TITULAR y/o sus representantes, según sea el caso, acepta todo el contenido de la presente y le concede(n) a AdC su autorización para que utilice dicha información personal conforme a las estipulaciones de la presente política, la cual también está publicada en la página web www.artesaniasdecolombia.com.co obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como TITULAR de datos personales.

- En el evento en que desee manifestar su negativa frente a la mentada autorización o solicitar la supresión de la información, podrá ejercer su derecho a través del correo: contactenos@artesaniasdecolombia.com.co o en cualquiera de los puntos de atención al ciudadano, dentro de los 30 días hábiles siguientes a la implementación y publicación de la Política de Privacidad y Protección de Datos Personales de AdC.

- Una vez vencido el periodo señalado anteriormente, el Instituto podrá mantener un tratamiento sobre los datos suministrados con anterioridad a esta legislación, en atención a lo consagrado en el numeral cuarto del artículo 10° del Decreto 1377 de 2013, sin perjuicio de la facultad que el TITULAR de la Información de ejercer en cualquier momento su derecho a pedir la eliminación del dato.

- No obstante, se hace la salvedad que de conformidad al artículo 9 del decreto 1377 del año 2013, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el TITULAR de esta, tenga un deber legal o contractual de permanecer en la base de datos de la entidad.

e. Por su parte, AdC asegura un manejo adecuado de los datos personales recolectados en sus bases de datos, registros de Ingreso a las instalaciones, registro fotográfico, firmas de asistencia, y de más medios de recolección, con el fin de proteger la privacidad de la misma y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del TITULAR, según lo estipulado en la ley. De esta manera la entidad manifiesta que garantiza los derechos de privacidad e intimidad en el tratamiento de los datos personales, en consecuencia, todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

f. Todas las personas que, en desarrollo de diferentes actividades, contractuales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar a AdC cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.

g. En efecto, AdC:

- Garantiza al TITULAR, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conserva la información bajo las condiciones de Seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realiza oportunamente la actualización, rectificación o supresión de los datos en los términos que estipula la ley.

- Actualiza la información reportada por los Encargados del Tratamiento en los términos que estipula ley.
- Tramita las consultas y los reclamos formulados por los TITULARES en los términos señalados en la ley.
- Se abstiene de circular información que esté siendo controvertida por el TITULAR y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permite el acceso a la información únicamente a las personas que pueden tener acceso a ello.
- Informa a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los TITULARES.
- Cumple las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

h. Cualquier consulta, reclamo o requisito debe ser dirigido a través de los diferentes sitios y canales de atención dispuestos por AdC para tal fin, los cuales se pueden consultar en la página web www.artesaniasdecolombia.com.co

10.14.2 A.18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

10.14.2.1 A.18.2.1 Revisión Independiente de la Seguridad de la Información

a. La Entidad, deberá realizar auditoría al Sistema de Gestión de Seguridad de la Información, con el fin de llevar a cabo la mejora continua.

10.14.2.2 A.18.2.2 Cumplimiento con las Políticas y Normas de Seguridad

a. Las políticas, procedimientos, y demás normatividad relacionada con seguridad de la información, implementada por AdC, es de obligatorio cumplimiento de servidores públicos, contratistas, pasantes, proveedores y terceros que por su naturaleza en su relación con la empresa tengan acceso a cualquier tipo de información.
b. Se debe asegurar por los directivos en cada área, la aplicación por parte de los empleados, de las políticas, los procedimientos y demás controles de seguridad de la información definidos por la empresa.

c. El incumplimiento a la Política de Seguridad y Privacidad de la información de la Entidad, traerá consigo, las consecuencias legales que apliquen a la normativa vigente.

10.14.2.3 A.18.2.3 Revisión de Cumplimiento Técnico

a. La oficina de tecnologías de la información, debe asegurar que se realicen revisiones periódicas a la implementación de las políticas y de los controles de seguridad de la información en los sistemas de información y los servicios tecnológicos.
b. La valoración de vulnerabilidades y las pruebas de penetración (Penetration Test) deben ser realizadas por personal idóneo para:

- Identificar fallos en las actualizaciones de los sistemas.
- Examinar la eficacia de los controles.
- Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para los sistemas y servicios tecnológicos.

c. De acuerdo con el resultado de la valoración de vulnerabilidades y las pruebas de penetración se debe tener en cuenta:

- Informar al responsable del activo, a la oficina de tecnologías de la información y al Oficial de Seguridad de la Información.
- Priorizar el tratamiento soportado en un análisis de riesgos.
- Documentar las acciones tomadas.
- Aplicar gestión del cambio.

10.15 VIIGENCIA DE LAS POLÍTICAS

Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de la misma.

11. NATURALEZA DEL CAMBIO

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Naturaleza del Cambio**
0		Publicación de la política inicial
1	21/Abril/2015	Ajuste a la política para incluir lineamientos de Gobierno en Línea
1	30/Marzo/2017	Ajuste a la política para incluir lineamientos de Gobierno en Línea
1	26/Diciembre/2018	Ajuste a la política para incluir la normatividad aplicable
2	10/Junio/2019	Ajustes para generar versión 2
3	06/Julio/2020	Se actualiza política con el anexo 1 protocolo de clasificación y rotulado
4	09/Septiembre/2020	Se aprueba el Política de seguridad y privacidad de la información.
5	26/Noviembre/2020	Se ajustó el documento identificando la nomenclatura del dominio y controles del anexo A de la norma ISO 27001:2013
6	26/Julio/2021	Se actualiza política, suprimiendo el anexo referente a Guía de rotulado y clasificación de información de AdC

Elaboró	Revisó	Aprobó
Angela Dorado Egas Especialista de Proyecto Oficina Asesora de Planeación e Información	**Johanna Paola Andrade** Profesional OAPI Oficina Asesora de Planeación e Información	**María Mercedes Sánchez** Jefe Oficina Asesora de Planeación e Información

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ARTESANÍAS DE COLOMBIA

ANEXO 1

GUÍA DE USO ACEPTABLE DE ACTIVOS

artesanías de colombia	**ANEXO 1** **POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**	Documento vigente a partir de: 2020/09/09 Versión: 1
		GUÍA DE USO ACEPTABLE DE ACTIVOS

1. OBJETIVO

Este documento describe los lineamientos para el uso aceptable de los activos de información en Artesanías de Colombia en adelante AdC, para garantizar la confidencialidad, integridad y disponibilidad de la información.

2. GENERALIDADES

Este documento describe las responsabilidades que tienen los usuarios frente al uso de los activos de información y los servicios tecnológicos provistos por AdC para cumplir con los requerimientos establecidos por el Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia la norma NTC/ISO 27001:2013.

Los activos de información que soportan los procesos de AdC, deben ser usados de manera adecuada, con el fin de preservar su seguridad de acuerdo con lo establecido en el presente documento y siguiendo los lineamientos de la NTC/ISO 27001:2013.

2.1 APLICACIÓN

La presente guía aplica para todos los servidores públicos, contratistas, proveedores, terceras partes o que, por su rol, tengan bajo su propiedad o custodia, activos de información de AdC.

Adicionalmente, para poder hacer uso de los recursos tecnológicos asignados, todo empleado debe diligenciar y aceptar los términos y condiciones establecidos en el formato definido para ello

3. DEFINICIONES

3.1 ACTIVO: Es todo aquello que posee valor para la organización o entidad, por lo tanto debe protegerse.

3.2 ACTIVOS DE INFORMACIÓN: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos de la entidad.

3.3 CLASIFICACIÓN DE LA INFORMACIÓN: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la organización.

3.3 CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

3.4 CUSTODIO: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado

3.5 DESKTOP: Computadora de escritorio u ordenador de sobremesa. Es una computadora personal que es diseñada para ser usada en una ubicación fija, como en un escritorio.

3.6 DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

3.7 HARDWARE: Componentes físicos del computador, es decir, todo lo que se puede ver y tocar.

3.8 INFORMACIÓN: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización o entidad.

3.9 SITIO: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)

3.10 INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos de información.

3.11 PROPIETARIO: Es el cargo responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.

3.12 REDES: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información

3.13 SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

3.14 SERVICIOS: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).

3.15 SOFTWARE: Todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos. (Sistemas operativos, aplicaciones, etc.)

3.16 UBICACIÓN: Lugar físico o electrónica en donde se localiza el activo identificado.

3.17 USUARIO: es un individuo que utiliza una computadora, un sistema operativo o cualquier sistema informático. Por lo general es una única persona.

4. NORMATIVIDAD APLICABLE

Ley 1712 de 2014

Decreto 1078 de 2015

Decreto 1080 de 2015

Ley 1581 de 2012

NTC/ISO 27001:2013

NTC/ISO 27005:2009

Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.

5. REGLA GENERALES DE USO

5.1 SERVICIO DE INTERNET

- Se debe utilizar internet para mejorar el conocimiento con relación a temas laborales, acceder a información técnica o científica, acceder a otras instituciones gubernamentales y en general, información que sea relevante para la entidad.

- Para la información consultada y utilizada de Internet se deben preservar los derechos de autor.

- La Oficina de tecnologías de la información debe establecer perfiles de navegación dependiendo de las responsabilidades laborales del usuario.

- Se prohíbe la descarga de archivos, programas o aplicaciones que no estén aprobadas por la Oficina de tecnologías de la información.

- La Oficina de tecnologías de la información debe configurar el navegador de los usuarios de manera segura.

- La Oficina de tecnologías de la información debe supervisar los anchos de banda, la disponibilidad, el uso del servicio de internet y debe mantener un registro de los sitios visitados.

- Se debe bloquear el acceso a cuentas de correos de tipo personal y nubes de almacenamiento no institucionales.

- La Oficina de tecnologías de la información debe definir listas negras de sitios de Internet no seguros a los que nadie debe tener acceso.

5.2 CORREO ELECTRÓNICO

- Se debe utilizar el correo electrónico para uso estrictamente laboral, compartir información técnica o científica, intercambiar información con otras instituciones gubernamentales y en general, intercambiar únicamente información que sea de relevancia para la entidad.

- Sí en los correos electrónicos se expresan opiniones personales debe aclararse que no son posición oficial de AdC.

- No se debe utilizar el correo electrónico para la trasmisión de amenazas, discriminaciones, hostigamientos, material obsceno o cualquier tipo de información que pueda afectar la integridad personal, la ética, el buen gusto y los derechos humanos.

- No se debe enviar información de la compañía a cuentas de correo personal, ni usar cuentas personales para temas oficiales.

- Todo usuario de correo debe tener implementada su firma y el aviso legal acorde al modelo oficial de ADC.

5.3 DISPOSITIVOS MÓVILES

Dispositivos móviles de la entidad

- Los dispositivos móviles de propiedad de la entidad (portátiles, celulares, tabletas, agendas, cámaras, relojes) son para uso estrictamente laboral, procesar o almacenar información técnica o científica, y en general, gestionar únicamente información que sea de relevancia para el cumplimiento de la misión y la visión de la entidad.
- Cuando los equipos portátiles sean autorizados para su retiro de la entidad, se debe poner un énfasis especial en su seguridad, para su traslado o estadía en un sitio externo, tales como aeropuertos, medios de transporte u hoteles, entre otros.
- Estos equipos deben contar con antivirus, firewall, tecnologías de cifrado, autenticación y control de integridad.
- Todos los equipos de cómputo en uso deben contar con software licenciado de acuerdo a la línea base de software autorizado.

Dispositivos móviles o fijos personales

El uso de los dispositivos personales debe cumplir con los requisitos establecidos en la guía de seguridad de la información para el teletrabajo, trabajo en casa y uso de dispositivos personales, debe además cumplir con los siguientes requisitos:

- Debe existir una justificación para su uso de acuerdo a las necesidades de su trabajo.
- La Oficina de tecnologías de la información verificará el que equipo cuente con por lo menos tres de los siguientes controles: antivirus, firewall, cifrado e integridad, controles de acceso y todo aquello que proteja la información reservada o sensible.
- Se utilizarán estándares de configuración específicos para cada dispositivo.
- Estos equipos deben contar con software licenciado
- No deben utilizar software que permita realizar ataques informáticos.

- La información de la entidad que se encuentre en los dispositivos debe estar respaldada.

- Los dispositivos deben estar actualizados con las últimas versiones de software.

- Se debe controlar la instalación de software en estos dispositivos.

- Se debe realizar un análisis de riesgo antes de permitir la conexión y uso de un dispositivo.

- Se deben establecer medidas técnicas en los equipos personales, para garantizar las mismas condiciones de seguridad de los equipos propios de la entidad.

- Los equipos personales no contarán con soporte técnico de la oficina de tecnologías de la información

5.4 EQUIPOS DE CÓMPUTO (DESKTOP)

Oficina de Tecnologías de la Información.

- Los equipos de cómputo deben estar ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado. Adicionalmente la entidad debe aplicar controles para mantener los equipos alejados de sitios que representan amenazas potenciales como: fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- Los equipos de cómputo críticos deben estar soportados por sistemas de potencia eléctrica regulada y estar protegidos por UPS.

- Es responsabilidad de la Oficina de Tecnologías de la Información capacitar al usuario en el manejo de las herramientas informáticas instaladas en el equipo de cómputo asignado, a fin de evitar incidentes de seguridad por mal uso.

- Todos los equipos de cómputo en uso deben contar con software licenciado de acuerdo con la línea base de software autorizado.

- Antes de entregar el equipo de cómputo al usuario, se debe garantizar que éste cuente con los requisitos mínimos de seguridad tales como: antivirus, firewall, entre otros.

- Las actividades de mantenimiento tanto preventivo como correctivo deben realizarse de acuerdo al cronograma establecido por la Oficina de Tecnologías de la Información.

- El mantenimiento preventivo, correctivo y soporte de los equipos de cómputo de la entidad, solamente los puede realizar el personal autorizado por la Oficina de Tecnologías de la información. Realizar este tipo de actividades a través de personas no autorizadas, se constituye en un incumplimiento de las políticas de seguridad y privacidad de la información.

- La información de la entidad que se encuentre en los equipos de cómputo debe estar respaldada.

- Cuando un equipo de cómputo vaya a ser reasignado o retirado de servicio, debe garantizarse un borrado seguro de toda la información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información.

- Los equipos de cómputo que requieran salir de las instalaciones de AdC para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información clasificada como reservada o sensible.

- El traslado entre dependencias de AdC de cualquier equipo de cómputo debe estar autorizado por el Grupo de Control de Activos y Almacenes para el debido control de inventarios.

- Cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deben ser autorizados por la oficina de tecnologías de la información.

Usuarios

- Los equipos de cómputo de propiedad de la entidad son para uso estrictamente laboral, procesar o almacenar información técnica o científica, y en general, gestionar únicamente información que sea de relevancia para el cumplimiento de la misión y la visión de la entidad.

- Los usuarios son responsables del buen uso y custodia de los equipos de cómputo asignados; en consecuencia, responderán por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- Alrededor de los equipos de cómputo no está permitido consumir alimentos o ingerir líquidos. El equipo de cómputo se debe mantener limpio y sin humedad.

- No está permitido colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

- Está prohibido llevar a cabo servicios de soporte o reparaciones en los equipos de cómputo, estas actividades deben ser ejecutadas únicamente por el personal autorizado por la Oficina de Tecnologías de la Información.

- Los usuarios no deben mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de estos, estas actividades deben ser ejecutadas únicamente por el personal autorizado por la Oficina de Tecnologías de la Información.

- El usuario está en la obligación de reportar cualquier incidente de seguridad de la información que se llegase a presentar con el equipo de cómputo asignado.

5.5 ALMACENAMIENTO EN LA NUBE

- Se prohíbe el uso de las nubes de tipo personal (One Drive, Dropbox, AWS entre otros) para el almacenamiento de información de AdC.

- El almacenamiento en la nube de la entidad es para uso estrictamente laboral, almacenar información técnica o científica y, en general, almacenar únicamente información que sea de relevancia para la entidad.

- La administración de la nube es responsabilidad de la Oficina de tecnologías de la información, teniendo en cuenta:

- Contar con acuerdo de confidencialidad con el proveedor.

- Contar con acuerdos de niveles de servicio con un 99.97% como mínimo.

- Contar con un procedimiento de gestión de usuarios de la nube. Estos usuarios deben ser autorizados por la Oficina de tecnologías de la información y el dueño de la información.

- Los canales de conexión a la nube deben ser seguros.

- Se debe realizar una autenticación segura.
- Se debe contar con contraseñas robustas de acceso a la nube.
- Las cuentas creadas deben tener una vigencia de 3 meses máximo.
- Establecer una gestión de capacidad y de disponibilidad de la nube.
- Si la información que va a ser almacenada es de carácter reservado o sensible, se deben implementar técnicas de cifrado y contar con la autorización del dueño de la información.
- Se deben establecer mecanismos de autenticación, autorización y registro para cada una de las actividades realizadas sobre el almacenamiento en la nube.
- Se debe respaldar la información almacenada en la nube.
- Se deben revisar los contratos de almacenamiento ofrecidos por el proveedor con el fin de no afectar la seguridad de la información.

6. NATURALEZA DEL CAMBIO

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Naturaleza del Cambio**
1	09/Septiembre/2020	Se crea la guía de uso aceptable de activos y se anexa a la Política de seguridad de la Información.

Elaboró	Revisó	Aprobó
Angela Dorado Egas Especialista de Proyecto Oficina Asesora de Planeación e Información	**Johanna Paola Andrade** Profesional OAPI Oficina Asesora de Planeación e Información	**María Mercedes Sánchez** Jefe Oficina Asesora de Planeación e Información