Agencia Nacional Digital

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. NOVIEMBRE 2025

Tabla de contenido

1. Introducción

La Corporación Agencia Nacional de Gobierno Digital —AND—, en la gestión de seguridad de la información establece condiciones adecuadas para la óptima operación de los activos de información y la infraestructura tecnológica que soporta los procesos de la entidad, para fortalecer la confidencialidad, disponibilidad, e integridad de la información. Así mismo propende por el cumplimiento de las directrices del Gobierno Nacional relacionadas con la seguridad y privacidad de la información, incluyendo la seguridad digital, ciberseguridad y la protección de los datos personales, el habeas data, manejo de la imagen de la entidad, de proveedores y terceros con los que la Entidad tenga vínculos aplicando metodologías de valoración y tratamiento de los riesgos según la normatividad vigente. El presente Manual de Políticas de Seguridad y Privacidad de la Información, es el documento donde se relacionan las políticas a desarrollar de manera detallada, clara y específica, para la protección de los activos de información que soportan los procesos de la entidad y que apoyan la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)

2. Objetivo

Establecer lineamientos para preservar la confidencialidad, integridad y disponibilidad de la información en la Corporación Agencia Nacional de Gobierno Digital —AND—, a través de la implementación del Sistema de Gestión de Seguridad de la Información y Privacidad de la Información, conforme al cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI con los requisitos legales, estratégicos, tácticos y operativos que aplican a la Entidad.

3. Alcance

Estas políticas, aplican a todos los niveles funcionales y organizacionales de la AND, a todos sus empleados de planta, contratistas, proveedores, y cualquier tercero que preste sus servicios, acceda, maneje o trate información de la Entidad, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la AND compartan, utilicen, recolectan, procesan, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, aplica a toda la información

creada, procesada o utilizada por AND, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. Definiciones

4.1 Términos asociados a seguridad de la información

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados (Ley 1712, 2014).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (Modelo de Seguridad y Privacidad de la Información, 2021).

Activo de Información: Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información sensible y/o importante para la JBB. (Ley 1712, 2014).

Amenaza: Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).

Análisis de riesgos: Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo. (Modelo de Seguridad y Privacidad de la Información, 2021).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley Estatutaria 1581. Art 3, 2012).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley Estatutaria 1581. Art 3, 2012).

Ciberseguridad: se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin.(Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020)

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Clasificación de activos: Se debe analizar cada activo de información para determinar los niveles de: confidencialidad, integridad y disponibilidad. Los parámetros a tener en cuenta para medir estos valores se definen en función a la clasificación de la información y nivel de servicios, teniendo como resultado el nivel de importancia de cada uno de los activos de información inventariados. (Ley 1712, 2014).

Confidencialidad: propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. (ISO/CEI 27000, 2018).

Control: Medida que modifica el riesgo. Sinónimo salvaguarda (ISO/CEI 27000, 2018).

Custodio: persona o entidad con la responsabilidad de proteger y vigilar un activo que se encuentra bajo su responsabilidad por efectos de su labor dentro de la entidad.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley Estatutaria 1581. Art 3, 2012)

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible son considerados datos públicos, entre otros, los datos relativos al estado civil de las

personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 Art 3, 2013).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley Estatutaria 1581. Art 3, 2012)

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 Art 3, 2013)

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (ISO/CEI 27000, 2018).

Encargado del Tratamiento de Datos: 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. (Ley Estatutaria 1581. Art 3, 2012).

Gestión de incidentes de seguridad de la información: Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/CEI 27000, 2018).

Gestión de riesgos: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (ISO/CEI 27000, 2018).

Incidente de seguridad de la información: único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información, (ISO/CEI 27000, 2018).

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712, 2014).

Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad (Ley 1712, 2014).

Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 (Ley 1712, 2014).

Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 (Ley 1712, 2014).

Integridad: La propiedad de salvaguardar la exactitud y complejidad de la información. (ISO/CEI 27000, 2018).

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Modelo de Seguridad y Privacidad de la Información, 2021).

Riesgo: La posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización. (ISO/CEI 27000, 2018).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/CEI 27000, 2018).

Seguridad digital: es la situación de normalidad y de tranquilidad en el entorno digital(ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley Estatutaria 1581. Art 3, 2012).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/CEI 27000, 2018)

4.2 Términos asociados a documentación y procesos administrativos

Archivo. Es el 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, 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. (Ley 1712, 2014).

Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (Ley 1712, 2014).

Documento de archivo. Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones. (Ley 1712, 2014).

5. Normatividad

La normatividad vigente en términos de seguridad de la Información se encuentra relacionada en las Política general de seguridad de la información de la Corporación Agencia Nacional de Gobierno Digital —AND—.

6. SOA actualizada SCD base

Las políticas de seguridad de la información y procedimientos definidas en este documento se alinean a los controles establecidos en la Declaración de Aplicabilidad, como parte del compromiso que tiene la Dirección de la AND para el SGSI.

7. Políticas de seguridad de la información y procedimientos

La Corporación Agencia Nacional de Gobierno Digital —AND—, establece a continuación, los siguientes lineamientos de seguridad y privacidad de la información, los cuales deberán ser cumplidos por todos los empleados de planta, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad.

7.1 Políticas de controles organizacionales

La Dirección General de la AND, que por medio de la Resolución No 35 DE 2023, establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Corporación Agencia Nacional Digital, dentro de su funciones tiene; "*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad y privacidad de la información"*, por lo cual establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración y buen uso de los activos de información, con el objetivo de garantizar su protección.

7.2 Gestión de las Políticas de Seguridad de la Información

a) La política general de seguridad de la información y las políticas específicas deben ser definidas, actualizadas, aprobadas por la Alta Dirección, publicadas y comunicadas a todas las partes interesadas que hacen parte de las operaciones de la AND.
b) La política general de seguridad de la información y las políticas específicas deben ser revisadas mínimo una vez al año por la Alta Dirección.
c) Cualquier cambio o actualización de la política general de seguridad de la información y/o políticas específicas deben ser realizadas con base al procedimiento de control de cambios establecido.

7.3 Roles y Responsabilidades de Seguridad y Privacidad de la Información

a) Para la gestión de la seguridad de la información se establece una estructura funcional en términos de roles y responsabilidades con base a la Política General de Seguridad y Privacidad de la Información en el capítulo de Organización de la Seguridad de la Información (Roles y Responsabilidades).

7.4 Segregación de Funciones

a) Para la gestión de la seguridad de la información se deben mantener la segregación de roles y funciones que eviten conflictos de interés y se mantenga la independencia frente a las responsabilidades.

7.5 Responsabilidades de la Dirección

a) La Alta Dirección de la AND debe exigir el cumplimiento de la seguridad de la información con base a la política general y específicas establecidas, así como de los procedimientos en su aplicación, promoviendo cláusulas contractuales, informando sus roles y funciones, manteniendo la sensibilización y control disciplinario frente a las acciones de los usuarios sobre su comportamiento.

7.6 Contacto con las Autoridades

a) El oficial de seguridad o el profesional de seguridad de la información debe mantener y documentar los contactos con autoridades (COLCERT, CSIRT, Policía, etc.) u otros especializados, con el fin de contactar en caso de que se presente un

incidente de seguridad de la información catalogado como grave o muy grave y requiera de asesoría externa.

7.7 Contacto con Grupos de Interés Especial

a) La AND, a través del Gestión de TI y Seguridad y Privacidad de la Información, así como el personal que se determine, deberán mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos, que permita la mejora continua del Sistema de Gestión de Seguridad de la Información- Digital de la Entidad.

7.8 Inteligencia de Amenazas

a) La AND debe recopilar y analizar el contexto de las amenazas de seguridad de la información con el fin de prevenirlas, detectarlas y/o dar respuesta oportuna frente a su materialización, reduciendo el impacto en sus operaciones.
b) La AND debe propender por mantener alineado el proceso de gestión de eventos e incidentes y la gestión de riesgos con las actividades de inteligencia de amenazas, con el fin de evitar posibles impactos a las operaciones de la Entidad.
c) Se debe promover la sensibilización y conciencia de las amenazas sobre la seguridad de la información en las partes interesadas de la AND.
d) La inteligencia de amenazas en seguridad de la información se considerará a nivel estratégico, táctico y operativo.
e) Se debe realizar la inteligencia de amenazas considerando todas las partes interesadas de la seguridad de la información en la AND, considerando partes internas y externas (proveedores, terceros, etc).

7.9 Seguridad de la Información en la Gestión de Proyectos

a) La seguridad de la información debe integrarse y gestionarse en todo el ciclo de la gestión de los proyectos.
b) Se deben definir requisitos de seguridad de la información para la gestión de los proyectos, de acuerdo al contexto y alcance de estos frente a las operaciones de la AND.
c) Se deben gestionar los riesgos, requisitos y controles de la seguridad de seguridad de la información definidos para el proyecto.

d) Se debe asegurar el acceso autorizado, transferencia y protección de la información en la gestión de los proyectos.
e) Cualquier cambio en los riesgos requisitos y controles de seguridad de la información del proyecto debe realizarse con base al procedimiento establecido y acordado entre las partes.
f) Se deben establecer y dar cumplimiento de los requisitos legales, contractuales y normativos de seguridad de la información exigidos en el proyecto.
g) Es responsabilidad de los supervisores de los proyectos y/o contratos que verifiquen los requisitos de seguridad de la información para los productos o servicios que entregará el proyecto, deben determinarse utilizando varios métodos, incluida la derivación de los requisitos de cumplimiento de la política de seguridad de la información, las políticas y las reglamentaciones específicas del tema. Así mismo otros requisitos de seguridad de la información de actividades como las revisiones de incidentes, uso de umbrales de vulnerabilidad o planificación de contingencias, asegurando así que la arquitectura y el diseño de los sistemas de información estén protegidos contra amenazas conocidas basadas en el entorno operativo.
h) Los supervisores de contratos, gerentes o responsables de los proyectos deben reportar en el caso de materialización los incidentes, eventos o riesgos de seguridad, con el fin de dar aplicar el procedimiento de notificación y gestión de incidentes de seguridad de la información y de la de Gestión de riesgos.
i) Es responsabilidad de los supervisores de los proyectos contar con el análisis y gestión de los riesgos de Seguridad y privacidad en la matriz correspondiente de la Entidad.

7.10 Inventario de Activos de Información

a) En la AND se deben identificar y mantener un inventario de activos de información con sus propietarios.
b) Los activos de información deben estar bajo la responsabilidad del dueño del activo para evitar conflicto y reducir oportunidades de modificación (intencional o no), no autorizada o mal uso de los activos de información.
c) Cualquier cambio en los activos de información debe ser promovido por el dueño del activo, analizado por el responsable de Seguridad de la Información y autorizado por ambas partes.
d) El inventario de activos de información debe mantener un control de acceso restringido sólo para las partes interesadas.

e) La publicación del inventario de activos debe darse de acuerdo con el contexto autorizado. Para el caso de exposición pública deben suprimirse los datos confidenciales de los activos de información.
f) El inventario de activos de información debe ubicarse, protegerse y almacenarse en los repositorios autorizados por la AND para tal fin.
g) Se debe revisar periódicamente, mínimo una vez al año, o cuando sea requerido el inventario de activos de seguridad de la información.

7.11 Uso Aceptable de Activos de Información

a) Los activos de la Corporación Agencia Nacional de Gobierno Digital —AND, deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, el proceso de Seguridad y privacidad de la información**,** con el acompañamiento permanente la Subdirección de Desarrollo y Servicios Ciudadanos Digitales , el proceso de Gestión de TI , el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y la Oficina Asesora de Planeación, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.
b) La AND, debe realizar revisiones periódicas de la información identificada y otros activos asociados contra el activo inventario mínimo una vez al año.

c) Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias o dueños de los activos que tienen la custodia de la información generada en el marco de su función se encargará de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca el proceso de Seguridad y privacidad de la información -AND.
d) La Subdirección Administrativa deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental- TRD, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física en la AND.
e) Los recursos de información de la AND solo pueden ser utilizados para fines autorizados relacionados con el desarrollo de actividades laborales y los objetivos

de la Entidad. Queda estrictamente prohibido el uso de los recursos para actividades personales o cualquier actividad que viole la ley, las políticas de la AND y los derechos de terceros.

f) Los empleados de planta, contratistas y proveedores que tengan acceso a la información de la Entidad, deben cumplir con todas las leyes, regulaciones y normas éticas aplicables en el uso de los recursos. Esto incluye el respeto a los derechos de autor, la privacidad de los datos, la confidencialidad de la información sensible y la prohibición de difamación, acoso, discriminación u otras conductas inapropiadas.
g) Los empleados de planta, contratistas y proveedores que tengan acceso a la información de la Entidad, deben respetar la privacidad de la información de la AND y no divulgar información confidencial o sensible a terceros no autorizados. Se deben seguir los lineamientos y procedimientos establecidos para el manejo y protección de la información confidencial. Todos deben firmar el formato acuerdo de confidencialidad y la AND, se reserva el derecho de monitorear y auditar el uso de los recursos de información para asegurar el cumplimiento de esta política y garantizar la seguridad de la información. Los usuarios deben estar conscientes de que el uso de los recursos puede ser monitoreado y registrado.
h) No se deben reutilizar documentos para impresión con datos personales, semiprivados, privados o sensibles o documentos catalogados como pública reservada o pública clasificada.
i) No se debe dejar desatendidos por parte de la Infraestructura tecnológica de la AND y sin ningún control de acceso documentos físicos, medios de almacenamiento externo (USB, discos duros, SD Card, CD, DVD, entre otros), Tokens y otros activos de información en los puestos de trabajo, oficinas, salas de reuniones o lugares de acceso público.

- **Responsabilidades de los Colaboradores Frente al Uso de los Servicios Tecnológicos**

Todos los empleados de planta o contratistas que hagan uso de los recursos tecnológicos de La Corporación Agencia Nacional de Gobierno Digital —AND—, tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimento de la misión de la Entidad. Para ello, deben acatar las siguientes disposiciones:

- **Del Uso de Correo Electrónico**

El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados de planta y contratistas del de La Corporación Agencia Nacional de Gobierno Digital cuyo uso se facilitará en los siguientes términos:

a) El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por Tecnologías de la Información, que cuenta con el dominio @and.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
b) El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la Entidad.
c) Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la validez de los mensajes de datos.
d) Se prohíbe el envío de correos masivos (más de 30 destinatarios) internos o externos, con excepción de las cuentas con permisos de Tecnologías de la Información y comunicaciones, así mismo los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
e) Todo mensaje de correo electrónico enviado por la Corporación Agencia Nacional de Gobierno Digital —AND—, mediante plataformas externas deberá hacerse con la cuenta de la Entidad y utilizando el dominio @and.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.
f) Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a Tecnologías de la Información la delegación del buzón correspondiente, relacionando los empleados de planta y contratistas que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.
g) Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente enviado a la carpeta no deseado, así como repórtalo a Tecnologías de la Información como incidente de seguridad, por los canales establecidos en la Entidad y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas

referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.

h) La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.
i) Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.
j) Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada de la Corporación Agencia Nacional de Gobierno Digital —AND—, a otras entidades o ciudadanos sin la debida autorización de la Dirección o las subdirecciones, así como previa revisión de Comunicaciones en caso de comunicados y Planeación para información Sectorial.
k) El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.
l) Está expresamente prohibido distribuir, copiar o reenviar información de la Corporación Agencia Nacional de Gobierno Digital —AND—, a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.
m) Cuando un empleado de planta o contratista cesa en sus funciones o culminar la ejecución de contrato con la AND, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de la Dirección, Subdirecciones o por orden judicial, por solicitud de Control Interno o temas de Control Disciplinario como parte de un proceso de investigación.
n) La AND, se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus empleados de planta o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa de la Dirección, supervisores del contrato, jefe inmediato, Gestión del Talento Humano a Gestión de TI. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los empleados de planta y contratistas que la AND realiza el referido monitoreo.

- **Del Uso de Internet**

Gestión de TI con el apoyo de Seguridad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los empleados de planta, contratistas y colaboradores las siguientes, entre otras:

a) Los servicios a los que un determinado usuario pueda acceder en internet dependerá del rol, funciones u obligaciones que desempeña en la AND y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.
b) Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
c) Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la Entidad.
d) Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
e) Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Corporación Agencia Nacional de Gobierno Digital —AND—, se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

- **Del Uso de los Recursos Tecnológicos**

Los recursos tecnológicos de La Corporación Agencia Nacional de Gobierno Digital —AND—, son herramientas de apoyo a las labores, responsabilidades y obligaciones de los empleados de planta y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

a) Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del empleado de planta o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Gestión de TI, salvo que medie solicitud formal de los directores, subdirectores a Gestión de TI.

b) Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, debe ser expresamente autorizado por Gestión de TI.
c) En caso de que el empleado de planta o contratista deba hacer uso de equipos ajenos a la AND, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red de la AND una vez esté avalado por Gestión de TI.
d) Los empleados de planta o contratista deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación laboral.
e) Los empleados de planta o contratista deberán utilizar las herramientas tecnológicas que proporcione Gestión de TI para gestionar la información digital de la AND.
f) No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y por ende, a la pérdida de la integridad de ésta.
g) No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por las subdirecciones.
h) Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor es Gestión de TI.
i) Gestión de TI realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.
j) La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es Gestión de TI, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
k) La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a Gestión de TI por el empleado de planta o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea suministrado por la AND, deberá reportarse a Gestión de TI siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.

l) La pérdida de información deberá ser informada con detalle a Gestión de TI y a Seguridad de la Información, como incidente de seguridad.
m) Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información física o digital deberá ser reportado a la mayor brevedad a Gestión de TI y Seguridad de la Información, por los canales establecidos en la Entidad, siguiendo los procedimientos establecidos.
n) Gestión de TI son los responsables de la administración del software desde la AND, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.
o) Todo acceso a la red de la Entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por Gestión de TI.
p) La conexión a la red Wifi en la AND, para empleados de planta y contratistas deberá ser administrada desde Gestión de TI; la autenticación deberá ser con usuario y contraseña.
q) La red Wifi para empleados de planta y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos en la Entidad.
r) Los equipos deben quedar apagados cada vez que el empleado de planta o contratista no se encuentre en su puesto de trabajo o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad.
s) Las herramientas corporativas instaladas en los dispositivos móviles que pertenecen a la AND serán gestionadas por Gestión de TI con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, garantizando el cumplimiento de la política general de seguridad de la Información. Así mismo el acceso al office 365 será controlado por el doble factor de autenticación.

- **Del Uso de los Sistemas, Herramientas de Información y Sistemas de Almacenamiento**

Todos los empleados de planta y contratistas de la Corporación Agencia Nacional de Gobierno Digital son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

a) Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los empleados de planta

y contratistas no deben revelarse a terceros, ni utilizar claves ajenas. De igual manera son responsables del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.

b) En ausencia del empleado de planta o contratista se debe reportar de inmediato, cualquier tipo de novedad, los accesos le serán bloqueados con una solicitud a Gestión de TI , con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista
c) Cuando un empleado de planta o contratista cesa sus funciones o culminar la ejecución de contrato con la AND, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente y todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información que estos ostenten será almacenada en los repositorios de la Entidad.
d) Todos los empleados de planta, contratistas, colaboradores y terceros de la entidad deben realizar el uso consciente de los sistemas de almacenamiento de información dispuestos por Gestión de TI, de esta manera son responsables de la información allí almacenada la cual debe ser estrictamente institucional y relacionada con sus actividades, obligaciones y funciones encomendadas asegurando su clasificación y los niveles de control de acceso requeridos para salvaguardar su integridad, disponibilidad y confidencialidad, así mismo de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

7.11 Devolución de Activos de Información

a) El personal y cualquier parte interesada que disponga de activos de información de la AND deben devolverlos en condiciones íntegras y aceptables al momento de cambio o término de relación contractual, convenio o acuerdo.
b) La devolución de los activos debe realizarse con base al procedimiento establecido o acordado entre las partes.
c) Se debe considerar la devolución segura de los activos en los contratos y/o acuerdos establecidos con las partes que tienen relación con la AND.
d) La AND, debe asegurar la devolución de activos de información por parte de los usuarios.

7.12 Clasificación de la Información

a) La información de la AND debe ser clasificada de acuerdo con las necesidades de seguridad de la información en términos de la confidencialidad, integridad, disponibilidad, requisitos legales y contractuales aplicables.
b) El dueño de los activos de información debe clasificar estos activos teniendo en cuenta el Procedimiento Gestión y Clasificación de Activos de Información AND.
c) El empleado de planta, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la Matriz Formato Registro de Activos de Información de la AND, con el apoyo de responsable de Seguridad de la Información o el profesional designado para su debido registro.
d) El empleado de planta, contratista, proveedor o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente, restringiendo la información, para proteger la integridad de la información y garantizar la disponibilidad, así como dar cumplimiento a los requisitos legales relacionados con la confidencialidad, integridad o disponibilidad de la información. De igual forma los activos distintos de la información están clasificados en el Formato Registro de Activos de Información-AND.

7.13 Etiquetado de la Información

a) La AND debe definir la forma del etiquetado de los activos de información de acuerdo con la clasificación establecida y medios que los contienen.
b) Los activos de información deben etiquetarse con base a la clasificación de la información establecida.
c) El dueño de los activos de información es responsable de etiquetar y fomentar el etiquetado de los activos de información en los custodios o delegados para uso.
d) Se deben etiquetar los activos de información en medios físicos, electrónicos y digitales.
e) Los activos de información que dispongan de etiquetado podrán ser considerados como públicos. Por tal motivo, es responsabilidad del dueño y usuarios mantener la aplicación oportuna de estos.

7.14 Transferencia de Información

a) La Corporación Agencia Nacional de Gobierno Digital —AND definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.
b) La AND firmará el Formato Acuerdo de Confidencialidad, con los colaboradores e incluirá una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información interna y confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.
c) Los empleados de planta o contratistas de la AND sólo podrán suministrar información a través de los canales o accesos seguros identificados en los anexos técnicos en los contratos o en los lineamientos de intercambio de información.
d) Ningún Empleados de Planta, Contratista o Terceros deben revelar o intercambiar información catalogada como pública clasificada y pública reservada, confidencial o privada, sin cumplir con el proceso formal de requisición de la información.
e) El intercambio o transferencia de información se debe realizar, teniendo en cuenta la normativa legal vigente aplicable.

7.15 Control de Acceso

a) La AND, debe implementar controles de acceso físico y lógico a la información de la entidad y otros activos asociados en relación a los requisitos con proveedores y de seguridad de la información para proteger el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.
b) Los propietarios o dueños de los activos de información, teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías (on premise o en nube) e infraestructura física (instalaciones y oficinas), todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información La Corporación Agencia Nacional de Gobierno Digital —AND.
c) La Entidad debe establecer lineamientos y procedimientos formales de control de acceso, con el fin de proteger la información y llevar la trazabilidad en cuanto uso por parte del personal autorizado.

d) Todos los empleados de planta o contratistas de la AND deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

7.16 Gestión de Identidad

a) La AND debe gestionar las identidades durante todo su ciclo de vida.
b) La creación de usuarios debe contar con una solicitud formal autorizada sobre las identidades por el responsable o dueño del activo.
c) El Líder de Gestión de TI asignará las credenciales iniciales y acceso según el perfil definido.
d) Cualquier cambio en funciones o responsabilidades debe derivar en una revisión de los permisos asignados por parte del responsable de Seguridad de la Información. Y el Líder de Gestión de TI deberá actuar en base a la aprobación del responsable del área solicitante.
e) La cuenta del usuario de acceso a cualquier activo de información debe ser deshabilitada inmediatamente al terminar o realizar un cambio en la relación laboral o contractual con cualquiera de las partes interesadas. Así mismo, todos los accesos, tokens, dispositivos o contraseñas asignadas deben ser recuperados o invalidadas.

7.17 Información de Autenticación

a) En la AND se debe asignar, gestionar y controlar la información de la autenticación a los activos de información.

Contraseñas

- Deben tener una longitud mínima de 12 caracteres y contener letras mayúsculas, minúsculas, números y caracteres especiales.
- Se deben cambiar periódicamente cada 30 días, o en un tiempo menor según el nivel de riesgo del activo de información.
- No se deben utilizar caracteres consecutivos en las contraseñas. Ej. 111, AAA, 123…
- No se debe utilizar información personal en uso de contraseñas.
- No se deben compartir las contraseñas.

- No se deben reutilizar contraseñas anteriores.
- Las contraseñas genéricas de ingreso inicial deben cambiarse inmediatamente.
- No deben almacenarse las contraseñas en texto plano en ningún sistema.
- Cualquier novedad con las contraseñas debe ser informada al dueño del activo y al responsable de Seguridad de la Información.

Tokens y dispositivos de autenticación

- Los tokens físicos y/o lógicos deben estar físicamente protegidos de acceso no autorizado
- Si se pierden o se detecta un posible compromiso, deben ser desactivados inmediatamente.
- El uso de tokens debe ser controlado y registrado.

Biometría

- Debe utilizarse únicamente cuando se garantice el cumplimiento de las normativas de protección de datos personales.
- Los datos biométricos deben almacenarse cifrados y con acceso restringido.

Certificados digitales y claves criptográficas

- Deben ser emitidos por una autoridad certificadora confiable.
- Las claves privadas deben mantenerse seguras y nunca compartirse.

7.18 Derechos de Acceso

a) Los derechos de acceso se concederán con base en el principio de mínimos privilegios, es decir, los usuarios sólo tendrán acceso a los recursos necesarios para cumplir con sus funciones.
b) El acceso a sistemas, datos o recursos deberá ser aprobado por el dueño del activo de información antes de su otorgamiento.
c) Todos los accesos deben ser registrados y documentados, incluyendo la solicitud, aprobación y asignación.
d) Se debe mantener una separación de funciones adecuada, evitando que una misma persona tenga permisos que puedan comprometer la seguridad (por ejemplo, desarrollo y aprobación en un proceso crítico).

e) Se debe llevar a cabo una revisión periódica de los derechos de acceso, al menos mensualmente, o según el nivel de riesgo del sistema.
f) Los derechos de acceso deben ser revocados o modificados inmediatamente cuando un usuario cambia de puesto, finaliza su relación con la AND o ya no necesita el acceso.
g) Se deben evitar cuentas genéricas o compartidas. En casos excepcionales donde se justifiquen, deben estar controladas, registradas y monitoreadas.
h) Los derechos de acceso otorgados a terceros deben estar limitados en alcance y duración, y sujetos a contratos que incluyan cláusulas de confidencialidad y seguridad.
i) Las solicitudes de acceso deben gestionarse a través de un proceso formal, documentado y auditable.
j) Debe mantenerse una trazabilidad de las acciones realizadas por los usuarios, mediante registros de auditoría (logs) que permitan verificar el uso correcto de los accesos otorgados.

7.19 Seguridad de la Información en las Relaciones con los Proveedores.

a) La Subdirección Jurídica deberá establecer en el momento de suscribirse contratos los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información en la AND.
b) La Subdirección Jurídica debe asegurar la inclusión de Cláusulas de Seguridad de la Información y Privacidad de los Datos Personales por parte de los Proveedores, permitiendo a la AND, revisar o auditar el cumplimiento de las políticas por parte de los proveedores
c) La Subdirección Jurídica deberá establecer lineamientos para el cumplimiento de las obligaciones contractuales en relación de Seguridad de la Información con terceros o proveedores.
d) La Subdirección Jurídica deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
e) La Gestión TI con el apoyo de la Seguridad de la Información deberán documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la AND.
f) La Gestión TI deberá verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.

g) Cualquier cambio en los servicios o ejecución de estos dentro del contrato o en los acuerdos de niveles establecidos entre las partes deben ser gestionados con el supervisor y realizar la gestión de cambios establecida.

7.20 Abordar la Seguridad de la Información en los Acuerdos con Proveedores

a) Todo contrato con proveedores que accedan almacenen, procesen o transmitan información de la AND debe incluir cláusulas específicas sobre seguridad de la información.
b) Los requisitos de seguridad en los contratos deben estar alineados con la clasificación de la información y el nivel de riesgo asociado al proveedor o servicio.
c) Las cláusulas de seguridad establecidas en los contratos deben ser revisadas por el responsable de Seguridad de la Información antes de la firma.
d) Se deben incluir disposiciones contractuales, como mínimo las siguientes:
- Confidencialidad y uso adecuado de la información
- Obligaciones ante incidentes de seguridad
- Protección de datos personales (si aplica)
- Controles de acceso físico y lógico
- Subcontratación y terceros
- Derecho de auditoría y monitoreo
- Responsabilidad por daños y perjuicios
- Eliminación o devolución de la información al finalizar el contrato.

e) Para proveedores críticos o de alto riesgo, se pueden requerir acuerdos específicos de nivel de servicio (SLA) que incluyan indicadores de cumplimiento de seguridad.
f) Todo contrato debe prever la posibilidad de auditorías o revisiones por parte de la AND o un tercero autorizado, para verificar el cumplimiento de las obligaciones de seguridad.
g) En caso de finalización del contrato, el proveedor debe eliminar o devolver toda la información de la AND de forma segura y documentada.
h) Los acuerdos deben contemplar la obligatoriedad de informar incidentes de seguridad que puedan afectar a la AND, en un plazo definido contractualmente.
i) Se debe incluir la posibilidad de actualización de las cláusulas de seguridad, en caso de cambios normativos o en los riesgos operacionales.
j) Todo proveedor debe firmar un acuerdo de confidencialidad antes de iniciar cualquier relación contractual, incluso en la etapa de negociación.

7.21 Gestión de la Seguridad de la Información en la Cadena de Suministro

a) Se deben identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información que puedan surgir de relaciones con terceros.
b) Antes de establecer una relación contractual con un proveedor o tercero, se debe realizar una evaluación de riesgos y capacidad de seguridad.
c) Los contratos deben incluir cláusulas específicas de seguridad de la información, incluyendo obligaciones de confidencialidad, medidas de protección, notificación de incidentes y derecho de auditoría.
d) Se debe establecer un proceso formal para la selección, evaluación y monitoreo de los proveedores, en función de su criticidad para la AND.
e) Cuando corresponda, se deben aplicar controles técnicos como la segmentación de redes, cifrado, monitoreo o acceso restringido a la información.
f) Las obligaciones de seguridad deben mantenerse durante toda la relación contractual y, si es necesario, después de su finalización (por ejemplo, cláusulas post-contractuales de confidencialidad o destrucción de información).
g) La AND debe contar con mecanismos para monitorear el cumplimiento de los acuerdos de seguridad por parte de los proveedores.
h) Los proveedores críticos deben ser incluidos en los planes de continuidad del negocio, en la medida que afecten la operación de la AND.
i) Debe establecerse un canal de comunicación formal con los proveedores para la gestión de incidentes de seguridad que puedan afectarlos o afectar a la AND.
j) En adquisiciones de software o hardware, se deben considerar prácticas seguras en la cadena de suministro tecnológica (por ejemplo, validación de origen, integridad del código, cumplimiento de estándares).

7.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores

a) Se debe monitorear, revisar, evaluar y gestionar periódicamente, mínimo cada mes, los requisitos de seguridad de la información y prestación de servicios.

7.23 Seguridad de la Información para el Uso de Servicios en la Nube.

a) La Corporación Agencia Nacional de Gobierno Digital —AND a través de los administradores de la infraestructura tecnológica será la encargada de mantener la seguridad y privacidad de la información y los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la Entidad, garantizando su continuidad, cumpliendo los niveles de servicio

requeridos aplicando las políticas y lineamientos definidos. Los contratos o convenios que impliquen el aprovisionamiento de servicios en la nube deberán incluir obligaciones para la prestación de servicios tecnológicos y aprovisionamiento de infraestructura, de cara a la mitigación de posibles riesgos.

b) El uso de los servicios de computación en la nube dispuestos en la Entidad debe ser exclusivo para el cumplimiento de las funciones u obligaciones encomendadas de los empleados de planta o contratistas, no está autorizado el uso de servicios de computación en la nube para fines personales.
c) Los administradores de la infraestructura tecnológica deben establecer mecanismos de autenticación, autorización y registro para cada una de las actividades realizadas sobre el almacenamiento en la nube.
d) La Gestión de TI y los administradores de la Infraestructura Tecnológica, implementaran estrategias para el respaldo de la información alojada en la nube.
e) La descarga de información de la nube en equipos personales con control de acceso no autorizados por parte de empleados de planta y/o contratistas será tratado como un incidente de seguridad de la información.

7.24 Planificación y Preparación de la Gestión de Incidentes de Seguridad de la Información

a) La AND establece un procedimiento formal para gestionar incidentes de seguridad, definiendo roles, responsabilidades, procedimientos, canales de comunicación y entrenamientos. Se deben realizar simulacros y mantener actualizado el plan de respuesta a incidentes.

7.25 Evaluación y Decisión sobre Eventos de Seguridad de la Información

a) En la AND todo evento de seguridad debe ser registrado y evaluado para determinar si constituye un incidente. Esta decisión se basa en criterios claros de impacto y riesgo, y debe estar documentada para su seguimiento y trazabilidad.

7.26 Respuesta a Incidentes de Seguridad de la Información

a) La AND debe tener procedimientos definidos para responder a incidentes, enfocándose en la contención, mitigación, recuperación y comunicación. Las acciones deben estar documentadas y alineadas con la gravedad del incidente.

7.27 Aprendiendo de los Incidentes de Seguridad de la Información

a) Después de cada incidente relevante, se deben identificar causas raíz y lecciones aprendidas. Esto permite mejorar los controles, actualizar procedimientos y prevenir recurrencias. Los hallazgos deben documentarse y comunicarse a la Alta Dirección si es necesario.

7.28 Recopilación de Evidencias

a) Durante la gestión de incidentes, se deben recopilar y preservar evidencias de forma legalmente válida, siguiendo cadenas de custodia, usando herramientas forenses y asegurando su integridad para posibles auditorías o acciones legales.

7.29 Seguridad de la Información Durante la Interrupción

a) La seguridad de la información debe ser integrada en los planes de continuidad del negocio y recuperación ante desastres.
b) Se deben identificar los controles críticos de seguridad que deben mantenerse activos durante la interrupción (ej. cifrado, autenticación, respaldo).
c) Durante la ejecución de planes de contingencia, se debe asegurar el acceso controlado a la información, especialmente si se opera desde ubicaciones alternas o remotas.
d) El personal involucrado en la respuesta a interrupciones debe estar capacitado para mantener las medidas de seguridad, incluso en condiciones de emergencia.
e) Los activos de información deben estar protegidos contra accesos no autorizados, pérdida, alteración o destrucción, incluso si los sistemas están degradados o en recuperación.
f) Cualquier uso de servicios alternos, proveedores o canales de comunicación durante la interrupción debe cumplir con los requisitos mínimos de seguridad definidos por la AND.
g) Finalizada la interrupción, se deben validar los sistemas y controles de seguridad antes de reanudar operaciones normales.
h) Todos los eventos, decisiones y medidas tomadas durante la interrupción deben ser documentados para evaluación posterior.

7.30 Preparación de las TIC para la Continuidad del Negocio

a) La infraestructura TIC debe estar alineada con los requisitos de continuidad del negocio, definidos por cada proceso crítico.
b) Deben existir planes de recuperación tecnológica (DRP) que contemplen respaldos, sitios alternos, alta disponibilidad y tiempos de recuperación definidos.
c) Las soluciones tecnológicas implementadas deben ser resistentes ante fallos y diseñadas para minimizar interrupciones.
d) Se deben realizar pruebas periódicas de los planes de continuidad y recuperación de TIC para asegurar su efectividad.
e) La información crítica debe ser resguardada y recuperable dentro de los tiempos y niveles de servicio establecidos (RTO/RPO).
f) El personal técnico debe estar capacitado y disponible para ejecutar las actividades de recuperación ante incidentes.
g) Debe asegurarse que los proveedores de tecnologías de la información y comunicaciones externos que soportan servicios críticos también cuenten con medidas de continuidad compatibles.
h) Todos los cambios o nuevas implementaciones tecnológicas deben considerar desde su diseño los aspectos de resiliencia y recuperación.
i) Se debe mantener documentación actualizada sobre procedimientos de recuperación, configuraciones y contactos clave.

7.30.1 Requisitos Legales, Estatutarios, Reglamentarios y Contractuales

a) En la AND se debe identificar, mantener actualizados y cumplir todos los requisitos legales, normativos y contractuales aplicables a la seguridad de la información, incluyendo leyes de protección de datos personales, ciberseguridad, propiedad intelectual y normativas del sector.
b) Todos los contratos con terceros deben incorporar cláusulas de confidencialidad y seguridad, y su cumplimiento debe ser monitoreado, documentado y verificado mediante auditorías periódicas.
c) Se deben implementar controles técnicos, organizativos y legales para prevenir incumplimientos, y ante cambios normativos, actualizar las políticas, procedimientos y contratos correspondientes.
d) Las obligaciones deben ser conocidas por los responsables, y cualquier incumplimiento debe ser reportado y tratado adecuadamente, manteniéndose registros que evidencien la conformidad.

7.31 Derechos de Propiedad Intelectual

a) La AND, se compromete a garantizar la identificación, documentación y cumplimiento de la legislación asociada a la seguridad de la información, incluyendo aquella relacionada con confidencialidad, protección de datos personales, los derechos de autor y la propiedad intelectual. Dentro de este propósito, se incluye velar por que el software instalado en los recursos de la plataforma tecnológica cumpla con los requisitos legales y de licenciamiento aplicables.
b) La AND, deberá realizar la actualización de la Matriz de Requisitos Legales para su control y seguimiento, con el apoyo del Oficial de Seguridad y Privacidad de la Información y el Oficial de Datos Personales, o quien haga sus veces, de acuerdo con lo establecido por el Gobierno Nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública.
c) La Subdirección Jurídica y los Líderes de Proceso serán responsables de determinar los lineamientos pertinentes de derechos de autor y propiedad intelectual sobre toda la información (documentos, diseños, códigos fuente, bases de datos, o demás activos de información), que se generen, notificando y dejando claro a todos los usuarios dicha propiedad en los diferentes contratos o convenios establecidos. Subdirección Jurídica de la Agencia.
d) Los empleados de planta y/o contratista, no deben descargar materiales sujetos a propiedad intelectual en los equipos de la AND.
e) La AND, deberá brindar definiciones y recomendaciones para la gestión, protección y exposición de los aspectos general desde propiedad intelectual - derechos de autor, con la finalidad de contribuir a su adecuado manejo al interior de la Entidad y promover la gestión del conocimiento, su posible protección y la gestión estratégica de la misma, en la aplicación de la guía establecida en el Sistema Integrado de Gestión de la AND.
f) Los contratos establecidos para el desarrollo de software por parte de contratistas de la AND o contratados con terceros deben especificar los acuerdos sobre propiedad, entrega y custodia del código fuente y sus respectivas versiones, documentación técnica y de uso del software o sistema de información, derechos de propiedad intelectual, incluir los soportes del desarrollo de las actividades establecidas. Implementar acciones que permitan dar cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

7.32 Protección de los Registros

a) Los registros deben ser identificados, clasificados y gestionados de acuerdo con su nivel de sensibilidad y valor legal o informativo.
b) Se debe garantizar la integridad, autenticidad y no repudio de los registros, evitando su alteración o destrucción no autorizada.
c) El acceso a los registros debe ser limitado y controlado con base en el principio de privilegio mínimo.
d) Se deben aplicar medidas de seguridad física y lógica según el medio en el que se almacenen los registros (papel, disco, nube, etc.).
e) Los registros deben ser conservados durante el tiempo requerido por normativas legales, contractuales o necesidades internas que aplican a la AND.
f) Se deben definir y aplicar procedimientos para su almacenamiento, respaldo y recuperación segura.
g) La eliminación de registros debe realizarse de forma segura y controlada, cumpliendo con los requisitos legales aplicables.
h) Deben mantenerse registros de acceso, modificación y eliminación para evidenciar su trazabilidad.
i) Se debe realizar auditorías y revisiones periódicas para verificar la correcta protección y gestión de los registros.
j) El personal debe ser capacitado sobre la correcta manipulación y protección de los registros.

7.33 Privacidad y Protección de Datos Personales

a) En la AND se gestiona la privacidad y protección de los datos personales con base a la política establecida, de acuerdo con el cumplimiento de los requisitos legales, contractuales y normativos vigentes.
b) La AND debe identificar y clasificar la información que contenga datos personales, obtener el consentimiento explícito de los titulares cuando sea legalmente requerido y asegurar que dicha información se utilice exclusivamente para los fines autorizados.
c) Se debe restringir el acceso a los datos personales únicamente al personal autorizado y capacitado, aplicar controles técnicos, físicos y administrativos para protegerla contra accesos no autorizados, pérdida o alteración, y conservarla solo por el tiempo necesario conforme a su finalidad o requerimientos legales.

d) Los datos personales deben ser eliminados o anonimizados de forma segura cuando ya no sea requerida, respetando en todo momento los derechos de los titulares (acceso, rectificación, cancelación y oposición).
e) La AND debe disponer de procedimientos de notificación y respuesta ante incidentes que comprometan la privacidad, capacitar regularmente a su personal en materia de protección de datos personales, cumplir con la legislación vigente y mantener registros que evidencien la correcta aplicación de esta política.

7.34 Revisión Independiente de la Seguridad de la Información

a) En la AND se debe revisar de manera independiente la seguridad de la información, mínimo una vez al año o cuando existan cambios representativos.
b) Las revisiones independientes de seguridad de la información deben ser realizadas por auditores internos o externos que no tengan relación directa con el área evaluada, garantizando objetividad, competencia e imparcialidad.
c) Estas revisiones deben evaluar la efectividad de los controles de seguridad, programándolos con base en el nivel de riesgo, la criticidad del proceso y los cambios recientes.
d) Los resultados, hallazgos y recomendaciones deben ser documentados y comunicados a la Alta Dirección, generando planes de acción correctiva para abordar cualquier desviación.
e) Las auditorías deben verificar el cumplimiento con la política de seguridad y otros requisitos aplicables, contribuyendo activamente a la mejora continua del SGSI y a la toma de decisiones estratégicas en materia de seguridad.

7.35 Cumplimiento de Políticas, Normas y Estándares de Seguridad de la Información.

a) En la AND se deben revisar periódicamente, mínimo cada mes o cuando sea requerido, el cumplimiento de las políticas, normas y estándares de seguridad de la información establecidas.
b) La AND debe establecer, comunicar y mantener actualizadas sus políticas, normas y estándares de seguridad de la información, asegurando que todos los usuarios con acceso a la información los conozcan y los cumplan.
c) Se debe realizar capacitación y sensibilización periódica en seguridad de la información, por lo menos una vez al semestre, y se evaluará el cumplimiento mediante auditorías, revisiones y controles.

d) Los incumplimientos deberán ser identificados, documentados, investigados y gestionados oportunamente, pudiendo derivar en sanciones disciplinarias, contractuales o legales, según su gravedad.
e) Cualquier excepción a las políticas deberá ser justificada y autorizada formalmente
f) La Alta Dirección tiene la responsabilidad de respaldar y promover el cumplimiento mediante liderazgo y asignación de recursos.

7.36 Procedimientos Documentados de Seguridad de la Información

a) La AND debe desarrollar, mantener y revisar periódicamente, mínimo una vez al año o cuando sea requerido, procedimientos documentados que describan claramente la aplicación de los controles de seguridad de la información definidos en sus políticas, asegurando que estos sean comprensibles, accesibles y adecuados al nivel de riesgo y complejidad de los procesos.
b) Cada procedimiento debe definir su propósito, alcance, responsables, actividades, entradas, salidas y controles asociados.
c) La divulgación debe hacerse de forma segura y controlada, garantizando que estén disponibles para quienes los aplican.
d) El personal debe recibir capacitación específica sobre su correcta aplicación, y se deben implementar mecanismos de control documental que aseguren la vigencia, trazabilidad y eliminación adecuada de versiones obsoletas.
e) La Alta Dirección debe asegurar los recursos necesarios para su implementación efectiva.

8. Políticas controles recurso humano

8.1 Comprobación de Antecedentes

a) La AND, durante el proceso de selección de personal de empleados de planta o contratistas, realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen, de acuerdo con la legislación, requisitos normativos, contractuales, clasificación de la información y riesgos identificados que aplican a la AND.

8.2 Seguridad de la Información Durante el Empleo

a) Toda relación contractual del personal de AND que manejen o tengan relación con activos de información incluirá responsabilidades de seguridad de la información y derechos legales sobre su propiedad o uso de acuerdo con su rol o cargo vigente.
b) Las funciones y responsabilidades de seguridad de la información serán comunicadas a las partes interesadas, a través de sus contratos, publicaciones, capacitaciones o instrucciones.

8.3 Concienciación, Educación y Formación en Seguridad y Privacidad de la Información

En la AND se fomentará la cultura organizacional en seguridad y privacidad de la información. Para esto:

a) La Corporación Agencia Nacional de Gobierno Digital —AND, definirá un "Plan de Sensibilización de Seguridad de la información y Protección de Datos Personales" a través de profesional de seguridad de la información y el apoyo de comunicación interna y externa de la AND, donde se planificará anualmente la manera en que se comunicarán recomendaciones o Consejo de seguridad de la información por diferentes medios a todos sus empleados de planta y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información, Datos Personales o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la Entidad. La creación de los contenidos se hará con apoyo de Gestión de TI y del profesional de Seguridad de la información.
b) La Corporación Agencia Nacional de Gobierno Digital —AND, a través de Talento Humano, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier empleado de planta y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, Gestión de TI con el apoyo del profesional de Seguridad de la Información apoyará en dichas inducciones.

8.4 Proceso Disciplinario

a) La AND establece el proceso disciplinario con control sobre el cumplimiento de la seguridad de la información por parte del personal. Por tal motivo, cualquier

incumplimiento de las políticas o requisitos de seguridad de la información establecidas en la AND y que han parte del rol o función, serán tratados con base al proceso mencionado.

Clasificación de Faltas de Seguridad de la Información

A continuación se pueden observar algunas de las faltas a nivel de seguridad por tipificación:

Faltas Leves

- No asistir a capacitaciones obligatorias sobre seguridad de la información.
- Retraso en la actualización de contraseñas sin comprometer sistemas críticos.
- Uso ocasional de dispositivos personales sin seguir políticas, sin exposición de datos sensibles.
- No aplicar etiquetas de clasificación de información en documentos internos.

Faltas Graves

- Compartir credenciales con terceros.
- No reportar incidentes de seguridad conocidos.
- Instalar software no autorizado en equipos corporativos.
- Uso indebido de servicios en la nube sin cumplir políticas.
- No garantizar la protección de datos personales conforme a la Ley 1581 de 2012.

Faltas Gravísimas

- Divulgación intencional de información confidencial o datos personales.
- Alteración o eliminación no autorizada de información crítica.
- Manipulación de sistemas para evadir controles de seguridad.
- Negligencia que provoque fuga masiva de datos o interrupción del negocio.
- Incumplimiento deliberado que afecte la continuidad del negocio o vulnere derechos de titulares de datos (Ley 1581 de 2012.

8.5 Seguridad de la Información en Cambio o Terminación del Empleo

a) En la AND se deben definir y comunicar las responsabilidades y obligaciones de seguridad de la información para el personal para cambios de rol o función, así

como para cuando se da la terminación del empleo o relación contractual o convenio con la Entidad.

b) Se deben mantener acuerdos de confidencialidad extendidos luego de la terminación del contrato, mínimo por 3 años, o de ser requerido por más tiempo dependiendo de los requisitos legales y normativos vigentes que apliquen según el caso.
c) Cualquier cambio de rol o función debe gestionarse en términos de la seguridad de la información con base al proceso establecido en la AND, evitando materialización de riesgos e incidentes.
d) Cualquier cambio o terminación del empleo debe ser reportado oportunamente por el jefe inmediato a Talento Humano, y este a su vez, al responsable de Seguridad de la Información, con el fin de tomar las acciones pertinentes para proteger la información, tales como (retiros oportunos de los activos de información), asegurar la continuidad de los accesos con la entrega segura de credenciales y la disponibilidad de la información con la entrega y Backups de los datos.

8.6 Acuerdo de Confidencialidad de la Información

a) Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar formato Acuerdo de Confidencialidad, así mismo de conocimiento y aceptación de las políticas definidas para la seguridad de la información.
b) Para efectos de acuerdos o convenios, se considerará como información confidencial todo dato, documento, material, conocimiento o cualquier otra información que atienda a los presupuestos del artículo 18 y 19 de la Ley 1712 de 2014 y que sea revelada al Receptor durante el curso de su relación laboral, contractual o de cualquier índole, exceptuando aquella que sea de dominio público acorde con el principio de máxima publicidad. La obligación de confidencialidad permanecerá en vigor en los términos previstos por la ley, independientemente de la razón de dicha terminación.

8.7 Política Trabajo a Distancia

a) La AND definirá las condiciones generales y de seguridad de la información para la implementación de la política de trabajo a distancia en casa y/o teletrabajo como herramienta estratégica de la transformación cultural de la Entidad, que corresponde a una modalidad organizacional del empleo.

b) Gestión de TI, apoyará la evaluación de los activos físicos y de información que estén vinculados a las actividades de trabajo a distancia y/o teletrabajo, con base en ello, realizar una evaluación de riesgos aplicada a esos activos, implementando los controles adecuados para mitigar y eliminar los riesgos identificados. Así mismo, apoyará en la verificación y configuración de las conexiones seguras que no impacten el desarrollo de las actividades de empleados de planta y contratistas en el cumplimiento de los objetivos de la Entidad.
c) El trabajo a distancia debe ser autorizado por la AND, sea a través de sus contratos y/o por el jefe Inmediato cuando sea requerido por necesidades operativas.
d) La AND proporciona canales y medios seguros para su conexión, tales como: VPNs, HTTPs, con sistemas de autenticación.
e) El personal autorizado para la modalidad de trabajo a distancia debe realizar sus labores en lugares seguros, evitando el acceso de personal no autorizado a los activos de información.
f) En el ejercicio de trabajo a distancia los usuarios deben cumplir con las políticas de seguridad de la información establecidas en este documento.
g) Cualquier riesgo, evento, vulnerabilidad, incidente de seguridad de la información durante el ejercicio del trabajo a distancia debe ser reportado de inmediato al jefe y al responsable de Seguridad de la Información, así como guardar la confidencialidad relacionada con el caso respectivo.
h) Los dispositivos utilizados para trabajo a distancia deben cumplir con los requisitos mínimos establecidos por la AND, especialmente, relacionados con sistemas de autenticación seguros, licenciamiento de software, antivirus vigente y actualizado, entre otros que se exijan.
i) No se debe almacenar información permanente en los dispositivos utilizados para el trabajo a distancia.
j) Se deben utilizar los repositorios autorizados por la AND para el almacenamiento de información.
k) El uso de dispositivos personales utilizados para el trabajo a distancia debe ser autorizado por la AND.
l) Para el caso de uso de dispositivos personales para el trabajo a distancia deben disponer de cuentas de usuario exclusivas para el ámbito laboral, independientemente de las personales y cumplir con los requisitos de seguridad mínimo exigidos por la AND.
m) La AND no se hace responsable del soporte y mantenimiento de equipos o dispositivos personales autorizados para el trabajo a distancia. De esta manera, los usuarios de estos deben realizar el soporte y mantenimiento idóneo que asegure la disponibilidad y seguridad de su herramienta de trabajo.

n) La AND, podrá realizar auditorías sobre los activos de información propios que hagan parte de sus operaciones, respetando el límite de uso personal de los equipos de los usuarios.
o) Las copias de seguridad de la información del trabajo a distancia se realizan en los repositorios autorizados de la AND. Cualquier dato que no se encuentre en estos es responsabilidad del usuario, frente a su disponibilidad como de la confidencialidad de este.
p) Toda información al finalizar el trabajo a distancia debe ser devuelta a la AND y ser eliminada de manera segura por parte de los usuarios, evitando cualquier fuga o pérdida de confidencialidad de la información.
q) La AND se reserva el derecho de revocar cualquier autorización, derechos de acceso y uso de equipos por parte de los usuarios.

8.8 Notificación de Eventos de Seguridad de la Información

a) La AND establece un canal de comunicación para el reporte de eventos, vulnerabilidades e incidentes de seguridad de la información de acuerdo con el procedimiento establecido
b) Todo el personal debe notificar o reportar los eventos, vulnerabilidades e incidentes de seguridad de la información de manera oportuna a través del canal autorizado.

8. Políticas de controles físicos

9.1 Perímetro de Seguridad Física

a) La AND debe mantener un perímetro de seguridad física alrededor de las instalaciones que albergan activos de información.
b) Se deben mantener paredes robustas, puertas de acceso con seguridad, según el nivel de criticidad de los activos protegidos.
c) Los puntos de entrada y salida de las instalaciones y áreas seguras de la AND deben estar claramente definidas, aseguradas y supervisadas.
d) Los perímetros de las áreas de la AND deben estar señalizadas, incluyendo advertencias sobre zonas restringidas y sistemas de vigilancia.
e) Se deben realizar revisiones periódicas, mínimo una vez al año, del perímetro para detectar vulnerabilidades y mejoras respectivas.

9.2 Controles Físicos de Entrada

a) Solo el personal autorizado podrá acceder a las áreas físicas donde se ubiquen activos de información.
b) Se deben implementar sistemas de control de acceso físico como tarjetas de proximidad, biometría o lectores de credenciales para el ingreso a las instalaciones o áreas seguras.
c) Todo acceso a las instalaciones y áreas restringidas debe ser registrado.
d) Los medios de acceso físico deben ser revisados periódicamente mínimo 2 veces al año y desactivados inmediatamente en caso de pérdida, renuncia o cambio de funciones.
e) El acceso de visitantes debe estar controlado, registrado y acompañado por personal autorizado.

9.3 Seguridad de las Instalaciones

a) Las áreas internas deben contar con controles físicos adecuados a su nivel de sensibilidad.
b) Se debe restringir el acceso a áreas críticas (centros de datos, cuartos de telecomunicaciones, centros de archivo físico).
c) Las puertas de acceso a las instalaciones, áreas internas y críticas deben mantenerse cerradas con llave o control electrónico cuando no estén en uso.
d) El mobiliario debe estar dispuesto de manera que evite la visualización no autorizada de la información (por ejemplo, evitar pantallas de computadoras frente a áreas comunes).
e) Se debe evitar el almacenamiento innecesario de información física o equipos fuera de zonas seguras.

9.4 Monitorización de la Seguridad Física

a) Las instalaciones deben contar con sistemas de monitoreo como cámaras de videovigilancia (CCTV), y alarmas.
b) La videovigilancia debe enfocarse en puntos de acceso, perímetros y áreas sensibles, sin invadir la privacidad de los colaboradores.
c) Las grabaciones deben almacenarse de forma segura durante el tiempo estipulado por la política interna o requisitos legales.

d) El monitoreo debe ser realizado por personal autorizado y capacitado, y con reportes a la unidad responsable de seguridad cuando sea requerido.
e) Cualquier anomalía detectada mediante los sistemas de monitoreo debe ser investigada y documentada como incidente de seguridad.

9.5 Protección Contra Amenazas Externas y Ambientales

a) La infraestructura física de la AND debe estar protegida contra amenazas físicas externas como incendios, inundaciones, terremotos y sabotaje.
b) Se deben instalar sistemas de detección y supresión de incendios (detectores de humo, extintores, rociadores automáticos) adecuados al tipo de instalación.
c) Los equipos críticos deben contar con protección contra fallos eléctricos, como UPS (sistemas de alimentación ininterrumpida) y generadores.
d) Se deben tomar medidas para controlar la temperatura, humedad y polvo en áreas seguras, especialmente, en los centros de cómputo, cuartos de telecomunicaciones y centros de archivo físico.
e) Deben existir planes de contingencia y evacuación ante emergencias físicas o ambientales, los cuales deben ser conocidos por las partes interesadas.

9.6 Trabajo en Áreas Seguras

a) Las áreas de la AND clasificadas como "seguras" (como centros de datos, centros alternos, cuartos de telecomunicaciones, centros de archivo físico), deben tener controles de acceso más estrictos que el resto de las instalaciones.
b) Solo personal previamente autorizado, validado y registrado podrá trabajar en estas zonas.
c) Deben definirse reglas claras sobre el ingreso y uso de dispositivos móviles, cámaras, memorias USB u otros equipos dentro de estas áreas.
d) Los trabajos realizados en áreas seguras deben ser supervisados y registrados, incluyendo tareas de mantenimiento o visitas técnicas.
e) Toda actividad sospechosa o acceso no autorizado en estas zonas debe reportarse inmediatamente y tratarse como incidente de seguridad.

9.7 Política Específica de Escritorio y Pantalla Despejados

a) Se debe guardar bajo llave la información considerada como confidencial o crítica (idealmente en una caja fuerte, gabinete u otra forma de mueble con seguridad)

cuando no se requiera, especialmente cuando se entregue la información por terminación de contrato; cada dependencia debe tener documentado en tablas de retención documental.

b) Es necesario proteger los dispositivos de punto final del usuario ejemplo mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o desesperado) dejar los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todos los equipos de cómputo y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático; reglas de bloqueo directorio activo o bloqueo local y socializarse.
c) La AND deberá realizar el buen uso de impresoras con una función de autenticación o control de acceso optimizando la reducción en el consumo de papel.
d) La AND deberá almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial, así mismo cuando ya no se necesiten, desecharlos mediante mecanismos seguros de eliminación.
e) Gestión de TI deberá establecer y comunicar reglas y orientación para la configuración de ventanas emergentes en las pantallas (p. ej., desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en un área pública); configuración de seguridad office 365 doble factor de autenticación.

9.8 Ubicación y Protección de los Equipos

a) Los equipos que procesan, almacenan o transmiten información deben ubicarse en lugares que minimicen los riesgos de acceso no autorizado, daño físico, interferencias o robos.
b) Se debe evitar, en lo posible, la ubicación de equipos cerca de ventanas, pasillos públicos o zonas con alto tránsito, para reducir la exposición.
c) Los dispositivos deben estar ubicados sobre superficies estables, lejos de fuentes de calor, humedad o vibración que puedan afectar su funcionamiento.
d) Los cables de energía, red y datos deben estar organizados, protegidos y ocultos siempre que sea posible, para evitar sabotajes, tropiezos o accesos no autorizados.
e) Los equipos deben estar anclados o asegurados físicamente en zonas críticas para prevenir su remoción no autorizada o robo.

f) En caso de equipos compartidos, se debe asegurar su uso correcto, mantenimiento y seguridad de la información.

9.9 Seguridad de los Equipos Fuera de las Instalaciones

a) Los equipos que se utilicen fuera de las instalaciones de la AND (teletrabajo, trabajo remoto), deben contar con las mismas medidas de protección física y lógica que dentro de las instalaciones.
b) Solo personal autorizado podrá retirar o usar equipos de propiedad de la AND fuera de las instalaciones.
c) Todo traslado o retiro de equipos debe registrarse previamente, incluyendo responsable, destino, duración y motivo del traslado.
d) Se debe evitar el almacenamiento de información sensible en dispositivos móviles o portátiles sin mecanismos de cifrado y autenticación.
e) El personal debe estar capacitado en buenas prácticas para el uso de equipos fuera de las instalaciones, incluyendo el resguardo físico durante el transporte y uso en sitios públicos.
f) En caso de pérdida, robo o daño de equipos fuera de las instalaciones, se debe reportar inmediatamente como incidente de seguridad.

9.10 Gestión de Medios de Almacenamiento Extraíbles

a) Los medios de almacenamiento o llaves criptográfica utilizados para gestión de información en la AND se deben almacenar en un entorno seguro y protegido de acuerdo con su clasificación de activo de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes.
b) Gestión de TI si es necesario por solicitud proteger la información en medios de almacenamiento extraíbles deberá usar técnicas criptográficas para la confidencialidad o la integridad de la información que son consideradas con críticas o importantes.
c) La AND dispone de herramientas colaborativas para almacenar múltiples copias de información valiosa que se encuentre en medios de almacenamiento separados para reducir aún más el riesgo de daño o pérdida de información con incidente.
d) Gestión de TI será el responsable de habilitar o bloquear los puertos de medios de almacenamiento extraíbles si existe una solicitud o por gestión de la seguridad o razón organizativa.

e) Gestión de TI deberá realizar eliminar datos de forma segura o formatear los medios de almacenamiento antes de utilizarlos, para minimizar el riesgo de fuga de información confidencial a personas no autorizadas.
f) La AND deberá tener el registro Baja de Bienes y/o en la recogida y eliminación de medios de almacenamiento propiedad de la Entidad en conformidad con el Manual Operativo para la Administración de Bienes de la AND y el diligenciamiento Formato correspondiente de Baja de Bienes.

9.11 Instalaciones de Suministro

a) La AND debe mantener la disponibilidad continua de servicios esenciales (energía eléctrica, telecomunicaciones, agua, climatización).
b) Las instalaciones eléctricas y de telecomunicaciones deben ser diseñadas y mantenidas conforme a estándares técnicos, evitando sobrecargas, interferencias o riesgos de seguridad de la información.
c) Se debe contar con sistemas de respaldo como UPS (sistemas de alimentación ininterrumpida), y plantas eléctricas alternas para áreas de procesamiento crítico (centros de datos, centros de telecomunicaciones, entre otras).
d) La infraestructura de suministro de servicios de energía eléctrica, telecomunicaciones, agua, climatización), deben estar protegidas contra accesos no autorizados, sabotaje o daño accidental.
e) Toda acceso y mantenimiento en las instalaciones de suministro debe estar autorizado por el responsable asignado, documentado y ejecutado por personal competente.

9.12 Seguridad del Cableado

a) Todo el cableado de energía, red, telecomunicaciones y datos deben estar protegidos física y lógicamente para evitar accesos no autorizados, daños o interferencias.
b) Siempre que sea posible, el cableado debe ser instalado en canaletas evitando la exposición en zonas de tránsito o acceso público.
c) Los puntos de conexión deben estar identificados y documentados claramente, sin permitir conexiones no autorizadas.
d) Deben realizarse inspecciones periódicas del cableado, mínimo una vez al año, para detectar previamente obsolescencia, manipulación, fallos técnicos o riesgos de seguridad de la información sobre este.

e) El cableado que transporta información debe estar cifrado.

9.13 Mantenimiento de los Equipos

a) Todos los equipos (PCs, servidores, telecomunicaciones, etc.), deben recibir mantenimiento preventivo y correctivo de forma periódica, mínimo una vez al año, o cuando se requiera, para asegurar su disponibilidad, integridad y confidencialidad.
b) Las actividades de mantenimiento deben ser planificadas, registradas y ejecutadas por personal autorizado o proveedores aprobados por la AND.
c) Durante las tareas de mantenimiento, se deben aplicar medidas para proteger la información contenida en los equipos (respaldo, desconexión, control de acceso físico, etc.).
d) No se debe permitir el retiro de equipos de las instalaciones para mantenimiento sin autorización formal por parte del responsable del activo, Gestión de TI y el responsable de Seguridad de la Información, y así mismo, disponer del registro de salida.
e) Cualquier componente reemplazado debe ser gestionado conforme a las políticas de eliminación segura.

9.14 Eliminación o Reutilización Segura de los Equipos

a) Antes de desechar, transferir o utilizar cualquier equipo que haya almacenado información, se deben aplicar un borrado o eliminación segura de los datos.
b) Se deben utilizar métodos aprobados de borrado seguro, sobreescritura múltiple o destrucción física (trituración, desmagnetización, etc.), según la criticidad de la información.
c) La eliminación o reutilización de equipos debe ser autorizada por Gestión de TI y el responsable de Seguridad de la Información.
d) Se debe mantener un registro de los equipos eliminados o reutilizados.
e) Ningún equipo con información sensible debe ser reutilizado por personal no autorizado sin asegurar su saneamiento completo.

9. Políticas de controles tecnológicos

10.1 Política de Configuración y Manejo Seguro de Dispositivos de Punto Final de Usuario

a) La AND protegerá la información que se recolecta, genere, procese o almacene en los dispositivos finales de los usuarios.
b) La política de configuración y manejo seguro de dispositivos de punto final de usuario será comunicada al personal de la AND.
c) Para las configuraciones de dispositivos finales de usuario se aplicarán controles de seguridad que protejan la información de la AND para cualquier tipo o clasificación de la información.
d) Se deben mantener registros o logs del uso de los dispositivos finales de los usuarios.
e) Se restringirá el acceso físico donde se encuentren los dispositivos finales de los usuarios y se dispondrá de protecciones físicas y ambientales.
f) Se restringirá la instalación de software en los dispositivos finales de la AND, sólo al uso de programas autorizados.
g) Cualquier instalación o cambio en el software de los dispositivos finales será realizado por Gestión de TI.
h) El uso de dispositivos finales en las instalaciones de la AND se restringirá a la conexión de redes de comunicaciones internas autorizadas. Para el caso de uso de estos en entornos fuera de las instalaciones, es responsabilidad de los usuarios la conexión a redes privadas seguras.
i) Los dispositivos finales de los usuarios dispondrán de sistemas de autenticación con usuario y contraseña robustos, sin exposición de información de registro.
j) Se configurará el cambio de contraseña de los equipos vinculados al dominio para periodos máximos de 30 días, o cambios extemporáneos cuando sea requerido.
k) Se configurará la restricción de acceso a 3 intentos fallidos a los dispositivos finales.
l) Se configurará la inactivación de sesiones de los dispositivos finales en 5 minutos.
m) Se deben cifrar los dispositivos finales o medios de almacenamiento que mantienen información crítica de las operaciones de la AND.
n) Los dispositivos finales dispondrán de un antivirus actualizado para protección de código malicioso.
o) Se restringirá la conexión de los dispositivos finales al uso de los servicios de telecomunicaciones y aplicaciones autorizadas por la AND.
p) Se monitorea y revisa el comportamiento de los usuarios frente al uso de los dispositivos finales.

q) Se restringirá el uso de dispositivos extraíbles en los dispositivos finales, mediante el bloqueo de puertos físicos (USB, sockets de memorias, entre otros).
r) Se mantendrán particiones en los dispositivos finales, el cual independicen los recursos del sistema operativo y aplicativos, frente a la información recolectada, generada o almacenada de las operaciones, con el fin de mantener la disponibilidad de la información frente a fallas propias del sistema. Dicha partición de almacenamiento de los datos deberá estar protegida de personal no autorizado, a través de mecanismos seguros como el cifrado de los datos.
s) Se restringirá el uso de sesiones simultáneas en los servicios de la AND que accedan en los dispositivos finales.
t) El uso de dispositivos personales será aplicado con base a la política establecida.
u) Las conexiones inalámbricas se realizan con base a los lineamientos establecidos en el uso aceptable de activos.

10.2 Gestión de Privilegios de Acceso

a) El acceso privilegiado a sistemas, aplicaciones y plataformas debe ser otorgado exclusivamente a usuarios autorizados por el responsable o propietario del activo de información, con base en funciones específicas.
b) Todo acceso privilegiado debe ser controlado, monitoreado, registrado y revisado periódicamente, mínimo una vez al mes por el responsable de Seguridad de la Información.
c) Las cuentas con privilegios elevados (administradores) deben ser asociadas o delegadas a una persona autorizada por el responsable del activo de información, no compartidas, y utilizar mecanismos de autenticación fuerte.
d) Los privilegios deben concederse bajo el principio de menor privilegio y retirarse tan pronto dejen de ser necesarios.
e) Cualquier uso indebido de privilegios debe ser tratado como un incidente de seguridad.

10.3 Restricción del Acceso a la Información

a) El acceso a la información debe ser controlado y restringido de acuerdo con la clasificación de la información y el rol del usuario.
b) Se deben utilizar listas de control de acceso (ACL), grupos de seguridad y perfiles de usuario para implementar controles de acceso lógico a los sistemas de información de la AND.

c) No se permite el acceso genérico o no autorizado a carpetas compartidas, bases de datos o sistemas de información.
d) Toda excepción debe estar documentada y autorizada por el responsable de seguridad o del sistema.
e) La información clasificada como privada o reservada debe estar protegida por mecanismos de cifrado, autenticación y control de acceso físico/lógico.

10.4 Acceso al Código Fuente

a) El acceso al código fuente de aplicaciones desarrolladas internamente debe estar restringido solo a desarrolladores autorizados.
b) Deben establecerse controles de autenticación, control de versiones y trazabilidad sobre cualquier modificación al código.
c) Todo acceso, descarga o extracción del código fuente debe quedar registrada y ser monitoreada.
d) No se permite el almacenamiento del código fuente en dispositivos personales, ni su envío por medios no autorizados.
e) Cualquier incidente relacionado con el código fuente debe reportarse y tratarse como una violación de seguridad.

10.5 Autenticación Segura

a) Todos los accesos a sistemas y servicios deben requerir autenticación mediante mecanismos e ingresos seguros.
b) Se deben implementar autenticación multifactor (MFA) para accesos privilegiados, servicios críticos o acceso remoto.
c) Las contraseñas deben cumplir con requisitos mínimos de longitud, complejidad, caducidad y almacenamiento seguro, de acuerdo con lo establecido en esta política para tal fin.
d) Las credenciales de acceso deben ser personales e intransferibles.
e) El intento de autenticaciones fallidas consecutivas debe generar alertas y bloqueos temporales o definitivos, según la política establecida.

10.6 Gestión de Capacidades

a) Gestión de TI debe monitorear y gestionar la capacidad de los recursos tecnológicos para asegurar la disponibilidad del servicio.

b) Se deben establecer umbrales de utilización y alertas para evitar saturaciones de servidores, redes, almacenamiento u otros componentes críticos.
c) Las decisiones de escalabilidad deben ser tomadas en base a análisis de tendencias y crecimiento de la demanda.
d) Se debe asegurar que los recursos puedan adaptarse oportunamente a los cambios de las operaciones de la AND o incremento de usuarios en los sistemas de información.

10.7 Controles de Código Malicioso

a) Todos los equipos de la AND deben contar con sistemas actualizados de detección y prevención de código malicioso (antivirus, entre otros que apliquen).
b) Se deben escanear frecuentemente archivos, correos electrónicos, descargas y medios extraíbles.
c) El acceso a sitios web maliciosos o sospechosos debe ser restringido mediante controles de navegación seguros (proxy, DNS filtering, etc.).
d) El personal debe estar capacitado para reconocer señales de infección y saber cómo actuar ante posibles incidentes.
e) Los registros de actividad de malware deben ser monitoreados y tratados por el Gestión de TI y el responsable de Seguridad de la Información.

10.8 Gestión de Vulnerabilidades Técnicas

a) Se debe identificar, evaluar y tratar las vulnerabilidades técnicas de sus sistemas y aplicaciones de la AND de forma continua.
b) Se deben ejecutar periódicamente, mínimo 2 veces al año o cuando sea requerido, análisis de vulnerabilidades internas y externas periódicamente, así como pruebas de penetración a los activos de información que soporten servicios críticos de la AND.
c) Las vulnerabilidades deben clasificarse por criticidad y corregirse oportunamente.
d) Se debe mantener informes de vulnerabilidades detectadas, su estado y responsables.
e) Todo proceso de remediación debe ser validado y documentado para asegurar su eficacia.

10.9 Gestión de la Configuración

a) La configuración de todos los activos tecnológicos debe ser gestionada de manera centralizada y controlada.
b) Se deben utilizar configuraciones seguras, validar las establecidas por defecto si cumplen con las necesidades de la AND y deshabilitar servicios innecesarios.
c) Las configuraciones deben documentarse, versionar y validarse antes de su despliegue en ambientes productivos.
d) Cualquier cambio en la configuración debe estar aprobado por el comité o área responsable para la gestión del cambio y ser registrado, respectivamente.
e) Las configuraciones deben ser auditadas periódicamente para asegurar el cumplimiento de los estándares definidos.

10.10 Eliminación Segura de la Información

a) Toda información que ya no sea necesaria debe ser eliminada de forma segura, considerando su nivel de clasificación.
b) La eliminación debe realizarse mediante métodos aprobados (borrado seguro, sobreescritura múltiple, cifrado con destrucción de claves, etc.).
c) La eliminación de datos debe ser documentada y, cuando corresponda, auditada.
d) El personal involucrado debe estar capacitado en los procedimientos adecuados para eliminar la información sin dejar rastros recuperables.

10.11 Enmascaramiento de Datos

a) Se deben aplicar técnicas de enmascaramiento de datos para proteger información sensible (privada o reservada), en ambientes de prueba, desarrollo o formación.
b) El enmascaramiento debe asegurar que los datos no puedan ser revertidos a su forma original sin autorización.
c) Solo personal autorizado podrá acceder a los datos reales no enmascarados.
d) Las políticas de enmascaramiento deben documentarse y aplicarse de forma consistente en todos los sistemas aplicables.

10.12 Prevención de Fugas de Datos

a) Se deben implementar controles de prevención de fuga de datos (DLP o relacionados), para detectar y evitar la exposición no autorizada de información.
b) Se debe monitorear el uso de medios extraíbles, correo electrónico, servicios en la nube y transferencias de archivos para identificar comportamientos riesgosos.

c) Toda salida de información sensible (privada o reservada), debe ser aprobada por el responsable o propietario en su rol o función, registrada y cifrada cuando corresponda.
d) Los incidentes o alertas generadas por los sistemas de prevención de fuga de datos deben ser analizados por el responsable de Seguridad de la Información o equipo delegado, y tratados conforme al protocolo.

10.13 Política de Respaldo

a) Gestión de TI deberá elaborar y gestionar un plan o bitácora de copias de información donde se identifique los registros precisos y completos de las copias de seguridad.
b) Gestión de TI deberá contar con un procedimiento de restauración documentado con medidas de respaldo para cubrir toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de un desastre en caso de sistemas y servicios críticos en el caso de requerir solicitar documentación a terceros.
c) El Procedimiento de restauración debe incluir el monitorear la ejecución de las copias de seguridad y abordar las fallas de las copias de seguridad programadas en la AND, para garantizar la integridad de las mismas
d) Gestión de TI será el responsable de almacenar las copias de seguridad en un lugar remoto seguro y protegido, a una distancia suficiente para escapar de cualesquiera daños por un desastre si se requiere.
e) Gestión de TI deberá realizar o solicitar a las terceras pruebas de restauración de las copias de seguridad y estar documentadas.
f) La AND, debe determinar los requisitos de copia de seguridad y cómo se aplican para los servicios en la nube, priorizando las copias de seguridad de la información, las aplicaciones y los sistemas de la entidad en el entorno del servicio en la nube.
g) Gestión de TI deberá por medio de los lineamientos de las Tablas de Retención Documental -TRD, cumplir con y el período de retención de la información lo esencial debe determinarse, teniendo en cuenta cualquier requisito para la retención de copias de archivo.

10.14 Redundancia de los Recursos de Tratamiento de la Información

a) La AND debe garantizar la disponibilidad continua de los recursos tecnológicos críticos mediante la implementación de mecanismos de redundancia apropiados.
b) Se deben identificar los sistemas, aplicaciones y servicios que requieren alta disponibilidad y establecer configuraciones redundantes (por ejemplo, servidores en clúster, balanceadores de carga, almacenamiento replicado, etc.).
c) Los elementos redundantes deben ser probados regularmente para verificar su funcionamiento y detectar posibles fallos.
d) La redundancia debe diseñarse de manera que no introduzca nuevos riesgos de seguridad o puntos únicos de falla.
e) La documentación técnica debe considerar configuraciones redundantes implementadas y los procedimientos de activación en caso de fallo del recurso principal.
f) La estrategia de redundancia debe estar alineada con el plan de continuidad del negocio y el análisis de impacto (BIA).

10.15 Política de Gestión de Registros

a) La AND, protegerá los registros (documentos, bases de datos, logs de auditoría), frente a afectación, pérdida, destrucción, alteración, acceso o divulgación no autorizada de acuerdo con los requisitos legales y contractuales vigentes.
b) Los registros deben ser clasificados en la AND, de acuerdo con al Procedimiento Gestión y Clasificación de Activos de Información y al programa de gestión documental, con los tiempos de retención, tipo de almacenamiento, controles de seguridad y demás elementos propios de este sistema de gestión.
c) Una vez terminado el tiempo de vida útil de los medios de almacenamiento de los registros o cuando la información ya no sea requerida por la AND, la información debe ser retirada y destruida dichos medios de manera segura de acuerdo con los lineamientos establecidos por Gestión Documental y Gestión de TI.
d) Los tiempos de retención, medios de almacenamiento, y tratamiento de los registros de la AND, de propiedad, responsabilidad o encargo, deben ser establecidos de acuerdo con la legislación vigente aplicable a través de las TRD.
e) La AND, podrá poner a disposición los registros a las diferentes autoridades judiciales que lo requieran para casos de investigación propia de casos que sean justificados. Así mismo, esos casos deben ser evaluados por la Subdirección Jurídica quien a su vez determinará el debido procedimiento frente a la disposición de los registros conservando el cumplimiento legal de la AND y la protección de los datos.

f) Cuando sea requerido entregar registros por orden judicial, la AND, realizará dicha entrega conservando la protección de esta de acuerdo con políticas y lineamientos establecidos y acordados con el ente judicial.
g) La infraestructura tecnológica deberá contar con la sincronización de relojes o que todos los sistemas tengan fuentes de tiempo sincronizadas permitiendo la correlación de registros entre sistemas para el análisis, alerta e investigación de incidentes.
h) La infraestructura tecnológica deberá tener configuraciones que permitan proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados. Así como la administración del control de acceso y privilegios.
i) Gestión de TI será responsable de la implementación de controles que deben tener como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro (fallas y alteraciones).
j) La infraestructura tecnológica deberá considerar el uso de técnicas Hashing criptográfico (proceso que genera un código único para representar un conjunto de datos.), así como el registro en archivos de solo lectura para la protección de los registros.
k) Gestión de TI es el único responsable de gestionar los registros en el caso que se requiera de auditoría, eventos y logs para recopilar, anonimizar retener o entregar evidencia que sea solicitada o que del análisis de infraestructura sea identificada.
l) Se deberá realizar análisis de los registros y tomar las medidas apropiadas de protección de la privacidad de los datos, así como, apoyar en la depuración o la resolución de errores, los registros que deben anonimizar cuando sea posible utilizando técnicas de enmascaramiento de datos que eviten obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la AND, antes de enviarlo al proveedor o quien los solicite previa aprobación de gestión de TI.
m) Se debe tomar medidas apropiadas de protección de la privacidad de los registros de eventos pueden contener datos confidenciales e información de identificación personal, así como realizar el análisis de los eventos que puedan representar indicadores de compromiso con la seguridad de la información.

10.16 Seguimiento de Actividades

a) Se deben registrar y monitorear las actividades relevantes de los sistemas de información para detectar accesos no autorizados, uso indebido o fallos.

b) Los eventos críticos como inicios de sesión, accesos privilegiados, modificaciones de configuraciones o eliminación de datos deben ser auditados.
c) Los registros deben estar protegidos contra alteraciones y accesibles únicamente al personal autorizado.
d) Se deben definir períodos de retención para los registros de acuerdo con requisitos legales y operativos.
e) La revisión de registros debe formar parte de la operación regular de seguridad y debe permitir la identificación de incidentes.

10.17 Sincronización del Reloj

a) Todos los sistemas de información críticos deben sincronizar sus relojes mediante servicios de tiempo real, relacionados con la hora colombiana.
b) La sincronización del tiempo debe asegurar la consistencia de los registros de auditoría en todos los sistemas.
c) Se deben usar múltiples fuentes de tiempo cuando sea posible, para asegurar redundancia y precisión.
d) La desviación de hora debe monitorearse y corregirse automáticamente para mantener la precisión.

10.18 Uso de Programas de Utilidad con Privilegios

a) El uso de programas utilitarios (como herramientas de administración del sistema, editores hexadecimales, analizadores de red, etc.), que requieren privilegios elevados debe estar estrictamente controlado.
b) Solo el personal autorizado de Gestión de TI podrá utilizar estas herramientas, previa justificación técnica.
c) Toda ejecución de estos programas debe ser registrada y su uso debe auditarse regularmente.
d) Las herramientas para el uso de programas utilitarios deben estar almacenadas en ubicaciones seguras, fuera del alcance de usuarios no autorizados.

10.19 Instalación del Software

a) La instalación de software aplica a para todos los equipos, sistemas operativos, máquinas virtuales, entornos Cloud (SaaS, PaaS, IaaS) y aplicaciones utilizadas

por la entidad. Incluye tanto el software base instalado para la ejecución de las actividades contractuales y funciones laborales.

b) Solo el personal autorizado de Gestión de TI podrá instalar software en los sistemas de la AND.
c) La instalación de software debe ser aplicada de acuerdo con el procedimiento de gestión de cambios establecido.
d) Todo software debe ser aprobado por el responsable de Seguridad de la Información, e implementado por Gestión de TI, validando fuentes legítimas para su uso.
e) Se deben utilizar mecanismos técnicos (como políticas de grupo, bloqueo de instalación), para restringir instalaciones no autorizadas.
f) El inventario de software instalado debe estar autorizado por el responsable de Seguridad de la Información y Gestión de TI, mantenerse actualizado y revisado periódicamente.
g) El control de la instalación se realizará con base a la política de control de software establecida en la Entidad.

Control del Software

- **Configuración Base Controlada**
  Todos los sistemas operativos institucionales serán desplegados a partir de las imágenes base validadas y configuradas por los proveedores procurando el mínimo software necesario para el funcionamiento de las aplicaciones institucionales.
- **Licenciamiento**
  La AND durante el proceso de adquisición de nuevo software se encargará de la gestión de licencias y permisos de uso.
- **Restricción de instalación**
  Los usuarios no tienen privilegios para instalar, modificar o eliminar software.
- **Responsabilidad de Instalación**
  Únicamente el área de infraestructura podrá realizar instalaciones, actualizaciones o desinstalaciones de software, de acuerdo con las necesidades operativas y los lineamientos de seguridad.
- **Aplicaciones de productividad**
  Toda aplicación de productividad, colaboración, gestión documental, y servicios en línea contratados o habilitados deberán ser autorizados formalmente antes de su habilitación y gestionada bajo cuentas institucionales y/o autorizadas por la AND.

Roles y Responsabilidades del Control del Software

ROL	RESPONSABILIDAD
Infraestructura	Instalar, actualizar y retirar software autorizado. Mantener la configuración base y mantener su seguridad.
Usuarios Finales	Usar únicamente el software aprobado y reportar necesidades o fallas que se produzcan.
Responsable de Seguridad de la Información	Validar que las configuraciones cumplan con las políticas de seguridad.
Oficial de Protección de datos personales	Verificar el cumplimiento a nivel de protección de datos personales.
Proveedores	Entregar software conforme a los requisitos técnicos y de seguridad definidos por la entidad.

Principios Rectores

- **Autorización previa:** Las máquinas en los ambientes de producción, preproducción y que deben tener un inventario asociado donde se relacionen los servicios instalados para cada uno de los servicios ciudadanos digitales.
- **Seguridad y cumplimiento:** Todo servicio debe cumplir con las políticas de ciberseguridad, protección de datos y estándares de gobierno digital.
- **Uso mínimo necesario:** Sólo se habilitarán las aplicaciones estrictamente requeridas para las funciones institucionales.
- **Prevención de Shadow IT:** Se prohíbe la creación o uso de cuentas en servicios cloud externos sin aprobación.
- **Gestión de Cambio:** Por medio de RFC se deben gestionar cada uno de los cambios realizados sobre cada una de las máquinas y sus ambientes.

Autorización de Uso

En el marco del proceso de seguridad y privacidad de la información cada solicitud de gestión de cambio del software deberá incorporar profesional en ciberseguridad quién contribuirá en la evaluación de la solicitud considerando:

- Clasificación de la información a manejar.
- Cumplimiento de normas de seguridad y protección de datos.
- Modelo de licenciamiento, contrato o condiciones de servicio.
- Riesgos asociados y medidas de mitigación.

Solo tras la aprobación del cambio se podrá:

- Realizar la instalación de software/aplicativo.
- Crear cuentas institucionales.
- Configurar accesos mediante autenticación corporativa.
- Integrar el servicio con otros sistemas institucionales.

Restricciones

No se permitirá el uso de software, servicios o aplicaciones no autorizadas (por ejemplo, almacenamiento en nubes personales, software libre no validado o herramientas sin contrato institucional).

Los usuarios no pueden registrar cuentas con correos institucionales en plataformas externas sin aprobación formal.

Está prohibida la instalación o ejecución de software local que interactúe con servicios cloud sin evaluación previa.

Buenas prácticas para el control del software

La entidad deberá procurar la implementación de buenas prácticas como:

- Uso de políticas de seguridad perimetral, antivirus y equivalentes según entorno para control y descubrimiento de aplicaciones.
- Inventario de aplicaciones/servicios de aplicaciones Cloud instaladas en cada una de las máquinas en los ambientes de producción, preproducción y QA.
- Integración de logs de uso con el SIEM institucional donde pueda realizarse monitoreo de los cambios en las configuraciones o aplicaciones.

- Aplicación de controles Zero Trust en el acceso a servicios Cloud.

10.20 Seguridad de Redes

a) Las redes que soportan los sistemas de información de la AND deben estar protegidas contra accesos no autorizados, ataques y uso indebido.
b) Se deben implementar medidas de seguridad como firewalls, segmentación, cifrado y monitoreo del tráfico de red.
c) Las configuraciones de dispositivos de red deben seguir lineamientos seguros y estar documentadas.
d) Se deben realizar pruebas periódicas de seguridad en la red para identificar vulnerabilidades.

10.21 Seguridad de los Servicios de Red

a) Todos los servicios de red (correo electrónico, DNS, VPN, etc.) deben estar configurados y protegidos conforme a buenas prácticas de seguridad.
b) Los servicios de red críticos deben contar con mecanismos de autenticación, cifrado y registros de auditoría.
c) Los servicios deben ser monitoreados para detectar accesos indebidos o fallos en la prestación.
d) Debe mantenerse un inventario de servicios de red habilitados, su propósito y responsables.

10.22 Segregación en Redes

a) Las redes de la AND deben estar segmentadas lógica o físicamente para separar ambientes críticos (producción, desarrollo, pruebas, administración).
b) Se deben aplicar políticas de firewall o VLANs para limitar el tráfico entre segmentos de red según la necesidad operativa y los principios de mínimo privilegio.
c) El acceso entre redes debe ser aprobado, registrado y monitoreado.
d) La segregación de redes debe revisarse regularmente y ajustarse según cambios en los sistemas o riesgos.

10.23 Filtrado Web

a) El acceso a internet debe ser controlado mediante sistemas de filtrado web para prevenir el acceso a contenidos maliciosos, inapropiados o no autorizados.
b) Se deben categorizar los sitios web y aplicar políticas de acceso según el perfil del usuario.
c) Todo intento de acceso a sitios bloqueados debe ser registrado y, cuando corresponda, analizado por el área de seguridad.
d) Las políticas de filtrado deben revisarse periódicamente para ajustarse a nuevas amenazas o necesidades del negocio.

10.24 Uso Criptografía

a) La AND, debe gestionar y proporcionar los recursos para la implementación de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad y disponibilidad. El cifrado de la información se realizará por solicitud de los usuarios o de manera general cuando así lo requiera la Entidad.
b) La AND, deberá realizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía, mediante las herramientas tecnológicas que se hayan definido y aprobado en la Entidad.
c) Gestión de TI es responsable de definir e implementar reglas desde la infraestructura para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas que cumplan con la reglamentación, políticas, estándares, guías aplicables en relación a proporcionar una protección adecuada a los equipos utilizados para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo. Así como proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.
d) La gestión de TI a través de la infraestructura tecnológica deberá realizar por solicitud de la administración de los sistemas de información o de usuarios específicos las gestiones necesarias para que la transmisión de información clasificada como reservada cuente con mecanismos de cifrado de datos. Adicionalmente establece los lineamientos de los controles criptográficos teniendo

en cuenta su uso para la protección de claves de acceso a sistemas, datos y servicios. Igualmente, para la información digital o electrónica reservada.

e) La AND, en casos de orden judicial, el cual debe entregar información para investigaciones de casos judiciales, debe acordar con el ente judicial realizar dicha entrega de manera cifrada cumplimiento con sus políticas de seguridad de la información y privacidad de los datos personales.
f) Los Empleados de planta, contratistas y terceros autorizados deben utilizar sólo las herramientas tecnológicas autorizadas por la Entidad para cifrar la información y gestión de las llaves criptográficas respectivas

10.25 Seguridad en el Ciclo de Vida del Desarrollo

a) Se debe integrar la seguridad de la información en todas las fases del ciclo de vida del desarrollo de sistemas y software.
b) Deben utilizarse metodologías de desarrollo seguras (como DevSecOps), que incluyan validaciones y controles específicos de seguridad.
c) El personal de desarrollo debe estar capacitado en prácticas seguras y en la identificación de vulnerabilidades comunes.
d) Toda nueva funcionalidad debe someterse a evaluación de riesgos antes de ser implementada.

10.26 Requisitos de Seguridad de las Aplicaciones

a) Deben definirse requisitos de seguridad desde el inicio de cada proyecto de desarrollo de aplicaciones o sistemas.
b) Los requisitos deben estar alineados con las políticas de seguridad y privacidad de la información, las leyes aplicables y los riesgos identificados.
c) Se deben considerar controles para autenticación, autorización, cifrado, manejo de errores, validación de entradas, entre otros.
d) Todo cambio en los requisitos de seguridad debe documentarse y validarse formalmente.

10.27 Arquitectura Segura de Sistemas

a) Toda solución tecnológica debe diseñarse con una arquitectura que incorpore principios de seguridad desde su concepción.

b) La arquitectura debe incluir controles de defensa en profundidad, segmentación, zonas de confianza y control de acceso.
c) Se deben realizar revisiones periódicas de la arquitectura para adaptarla a nuevas amenazas y requisitos de las operaciones.
d) Los componentes utilizados deben provenir de fuentes confiables y no deben presentar vulnerabilidades conocidas.

10.28 Codificación Segura

a) Todo desarrollo debe seguir prácticas de codificación segura basadas en estándares reconocidos (como OWASP, etc.).
b) Se deben evitar errores comunes como inyecciones, desbordamientos, manejo inadecuado de sesiones o falta de validación.
c) El código debe ser revisado y auditado para detectar vulnerabilidades antes de ser promovido a producción.
d) El análisis estático y dinámico debe integrarse en el proceso de desarrollo.

10.29 Pruebas de Seguridad en Desarrollo y Aceptación

a) Las aplicaciones y sistemas deben ser sometidos a pruebas de seguridad antes de su puesta en producción.
b) Las pruebas deben incluir técnicas como escaneo de vulnerabilidades, pruebas de penetración, entre otras, según el caso.
c) Todo hallazgo debe ser registrado, clasificado por criticidad y tratado antes del despliegue.
d) Se debe realizar una validación de seguridad posterior a cualquier cambio importante en la aplicación o infraestructura.

10.30 Externalización del Desarrollo

a) El desarrollo de software realizado por terceros debe estar sujeto a los mismos requisitos de seguridad que el desarrollo interno.
b) Los contratos con proveedores deben incluir cláusulas específicas sobre la protección del código, la propiedad intelectual y la confidencialidad.
c) La AND se reserva el derecho de auditar y revisar el código desarrollado por terceros.

d) Todo desarrollo externo debe ser validado por el equipo de Gestión de TI y el responsable de Seguridad de la Información o equipo delegado, antes de su implementación.

10.31 Separación de los Ambientes de Desarrollo, Prueba y Producción

a) Los ambientes de desarrollo, prueba y producción deben estar completamente separados para evitar impactos cruzados y riesgos de seguridad.
b) No se permite el uso de datos reales para ser utilizados en ambientes de desarrollo o pruebas. En caso de ser requerido debe ser autorizado por el responsable del activo y el responsable de Seguridad de la Información, y en su aplicación estar anonimizados o enmascarados.
c) Los accesos a cada ambiente deben estar controlados y diferenciados según el rol del usuario.
d) Los cambios entre ambientes deben seguir procedimientos controlados y aprobados.

10.32 Gestión de Cambios

a) Todo cambio en la infraestructura, software o configuración debe estar debidamente planificado, aprobado y documentado.
b) Se debe evaluar el impacto del cambio en la seguridad y privacidad de la información antes de su implementación.
c) La gestión de cambios debe incorporar pruebas y respaldos de los datos.
d) Los cambios deben ser registrados y revisados periódicamente.

10.33 Datos de Prueba

a) Los datos utilizados en pruebas deben ser ficticios o enmascarados si provienen de información real, previamente autorizada por el responsable del activo y el responsable de Seguridad de la Información.
b) No se permite el uso de datos personales reales o confidenciales en ambientes de prueba.
c) Los datos de prueba deben ser gestionados, almacenados y eliminados de manera segura.

10.34 Protección de los Sistemas de Información Durante las Pruebas de Auditoría

a) Las pruebas de auditoría, escaneos de seguridad o revisiones técnicas deben planificarse considerando no afectar la operación de los sistemas evaluados.
b) Las pruebas deben ser autorizadas previamente por la Dirección de la AND o su delegado en el proceso respectivo, y coordinadas con las áreas técnicas respectivas.
c) Se deben aplicar medidas para proteger la integridad, disponibilidad y confidencialidad de los sistemas durante las pruebas.
d) Todo resultado debe ser tratado con confidencialidad y utilizado solo para fines de mejora de seguridad.

10. Cumplimiento y Sanciones

Las políticas de seguridad y privacidad de la información son de cumplimiento obligatorio por todo personal (interno y externo), áreas, subdirecciones que tenga un vínculo o relación contractual con la Corporación Agencia Nacional de Gobierno Digital —AND.

Cualquier incumplimiento de estas políticas podrá ser motivo de evaluación por parte de la Entidad con base a su proceso disciplinario establecido.

La falta de conocimiento de los presentes lineamientos no libera a los empleados de planta, contratistas y colaboradores de la Corporación Agencia Nacional de Gobierno Digital —AND, de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de tecnología o por el incumplimiento de los lineamientos aquí descritos.

Cualquier violación a las políticas de seguridad de la información de la Corporación Agencia Nacional de Gobierno Digital —AND debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

Gestión de TI, será la encargada de recopilar y entregar las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno a quien corresponda, así mismo será el encargado o dueño del activo de registrar y gestionar el Incidente de seguridad con el incumplimiento de las políticas con el apoyo del profesional de Seguridad cuando se requiera.

11. Documentos de referencia

De acuerdo con la política general se asocian los siguientes documentos de referencia:

- Norma ISO 27001:2022. Sistema de gestión de seguridad de la información. Requisitos.
- Norma ISO 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- Política general de seguridad y privacidad de la información.
- Normograma.

12. Responsables del proyecto en la entidad

Para asegurar una comunicación efectiva y transparente a lo largo del proyecto, se acordó establecer un diálogo continuo que permita resolver de manera directa y oportuna cualquier duda que surja. El Ministerio TIC designó al profesional Jonnathan Páez Lozano como responsable principal del Anexo 01 – Operación, soporte y seguridad**.** Su labor consiste en mantener informados a todos los involucrados en el proyecto y gestionar los temas que se presenten, facilitando así la coordinación de actividades y el logro de los objetivos.

Cargo	Entidad	Rol
Directora de Gobierno Digital	Ministerio TIC	Supervisor convenio
Coordinador GIT de SCD de la Dirección Gobierno Digital	Ministerio TIC	Representante del comité operativo
Gerente de Proyecto	Ministerio TIC	Responsable Anexo 1 – Apoyo a la Supervisión
Subdirectora SCD	Agencia Nacional Digital	Supervisor AND

Cargo	Entidad	Rol
Líder técnico	Agencia Nacional Digital	Líder técnico
Líder anexo 1	Agencia Nacional Digital	Líder anexo 1
Administrador	Agencia Nacional Digital	Administrador

Tabla 3 responsables del proyecto en la entidad

9. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	13/10/2020	Emisión del documento
2	12/08/2022	Cambio del objetivo, alcance, incorporación de definiciones, descripción de obligaciones por componente de seguridad de la información. De igual manera, se hacen ajustes en el apartado de las responsabilidades, uso y apropiación y vigencia de la política.
3	13/12/2023	Se incluyen roles, responsabilidades del SGSI. Se actualizan los lineamientos de Seguridad de la información y privacidad de los datos personales en la gestión de proyectos. Se incluyen las autoridades con que se deben tener contacto en caso de incidentes y recepción de actualizaciones de seguridad. Se incluyen lineamientos para el uso de equipos personales. Se incluyen lineamientos de seguridad de la información en el proceso de selección del talento humano. Se incluye la política de uso aceptable de los activos. Se incluye lineamientos de etiquetado de activos de información
4	4/02/2025	Se actualiza al cumplimiento del estándar ISO/IEC 27001:2022

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
		Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información y ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información
5	04/12/2025	Se complementan lineamientos de seguridad con base a las buenas prácticas de la ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Se estandariza el nombre del manual con la política general de seguridad y privacidad de la información. Se incluyen la política de control de software y las faltas en la política de control disciplinario.

Elaboró	Revisó	Aprobó
Lady Gilary Torres Becerra Contratista - Gerente Anexo 01 Subdirección de Desarrollo y SCD	Julio Ernesto Echavarria Poveda Subdirector de Desarrollo y SCD Maricela Torrenegra Barrios Profesional de Planeación (E)	Adriana Garcés Ruiz Directora AND