CONTENIDO

1. INTRODUCCÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. DEFINICIONES 4
5. NORMATIVIDAD. 8
6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 8
6.1. POLÍTICAS DE CONTROLES ORGANIZACIONALES. 8
6.1.1. Organización de Seguridad Digital y Privacidad de la Información. 8
6.1.2. Uso Aceptable de la Información y Otros Activos Asociados 10
6.1.3. Clasificación de la Información. 11
6.1.4. Transferencia de Información. 12
6.1.5. Control de Acceso. 13
6.1.6. Seguridad de la Información en la Relaciones con los Proveedores. 13
6.1.7. Seguridad de la Información para el Uso de Servicios en la Nube. 14
6.1.8. Política Específica Sobre la Protección de los Derechos de Propiedad Intelectual. 15
6.2. POLÍTICAS CONTROLES RECURSO HUMANO 16
6.2.1. Política Trabajo a Distancia 16
6.3. POLÍTICAS DE CONTROLES FISICOS 16
6.3.1. Política Específica de Escritorio y Pantalla Despejados 16
6.3.2. Gestión de Medios de Almacenamiento Extraíbles 17
6.4. POLÍTICAS DE CONTROLES TECNOLOGICOS 18
6.4.1. POLÍTICA CONFIGURACIÓN Y EL MANEJO SEGUROS DE LOS DISPOSITIVOS DE PUNTO FINAL DEL USUARIO. 18
6.4.2. Política de Respaldo 18
6.4.3. Política de Gestión de Registros 19

6.4.4. Uso Criptografía 21
6.5. RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS. 22
6.5.1. Del Uso de Correo Electrónico. 22
6.5.2. Del Uso de Internet 25
6.5.3. Del Uso de los Recursos Tecnológicos 25
6.5.4. Del Uso de los Sistemas, Herramientas de Información y Sistemas de Almacenamiento 28
7. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN 29
7.1. Capacitaciones en Seguridad Digital 29
8. CUMPLIMIENTO Y SANCIONES 29
9. CONTROL DE CAMBIOS 30

1. INTRODUCCÓN

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, seguridad digital, 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 Digital y Privacidad de la Información, es el documento donde se relacionan las políticas a desarrollar de manera detallada, clara y especifica, 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, recolecten, procesen, 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

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).

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).

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 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)..

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).

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

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)

5. NORMATIVIDAD.

La normatividad de 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. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Corporación Agencia Nacional de Gobierno Digital —AND—, establece a continuación, los siguientes lineamientos de seguridad Digital 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.

6.1. 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 digital y 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.

6.1.1. Organización de Seguridad Digital y Privacidad de la Información.

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

h) 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.

i) 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.

j) 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.

6.1.2. Uso Aceptable de la Información y Otros Activos Asociados

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 se seguridad digital asociados contra el activo inventario mínimo una vez a 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 encargarán 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 los 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 publica 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.

6.1.3. Clasificación de la Información.

a) El dueño de los activos de información debe clasificar estos activos teniendo en cuenta la Procedimiento Gestión y Clasificación de Activos de Información AND.

b) 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 Oficial de Seguridad de la Información o el profesional designado para su debido registro.

c) 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 está clasificada en el Formato Registro de Activos de Información-AND.

d) El dueño de los activos de información debe etiquetar los activos teniendo en cuenta las Tablas De Retención Documental

6.1.4. 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 solo podrán suministrar información a través de los canales o acceso 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.

6.1.5. Control de Acceso.

a) 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.

b) 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.

c) 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.

d) 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.

6.1.6. Seguridad de la Información en la 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.

6.1.7. 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.

6.1.8. Política Específica Sobre la Protección de los 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 organización.

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.

6.2. POLÍTICAS CONTROLES RECURSO HUMANO

6.2.1. Política Trabajo a Distancia

a) La AND, definirá las condiciones 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, apoyara 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.

6.3. POLÍTICAS DE CONTROLES FISICOS

6.3.1. 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.

6.3.2.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 criticas 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 razón organizativa

e) Gestión de TI deberá realizar eliminar datos de forma segura o formatear los medios de almacenamiento antes de reutilizarlos, 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.

6.4. POLÍTICAS DE CONTROLES TECNOLOGICOS

6.4.1. POLÍTICA CONFIGURACIÓN Y EL MANEJO SEGUROS DE LOS DISPOSITIVOS DE PUNTO FINAL DEL USUARIO.

6.4.2. 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 los 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.

a) Gestión de TI deberá realizar o solicitar a las terceras pruebas de restauración de las copias de seguridad y estar documentadas.

b) 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.

c) 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 l esencial debe determinarse, teniendo en cuenta cualquier requisito para la retención de copias de archivo.

6.4.3.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 destruido 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 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) Infraestructura tecnológica 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 anonimizarse cuando sea posible utilizando técnicas de enmascaramiento de datos obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlo al proveedor o quien los solicite previa aprobación de gestión de TI.

m) Infraestructura Tecnológica 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.

6.4.4.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) 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 que 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 solo las herramientas tecnológicas autorizadas por la Entidad para cifrar la información y gestión de las llaves criptográficas respectivas

6.5. 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:

6.5.1. 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 Gestión de TI, 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 Gestión de TI, 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 Gestión de TI 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 Gestión de TI 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 culmina 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.

6.5.2. 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 dependerán 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.

6.5.3.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.

6.5.4. 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 revelarlas 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 culmina 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 consiente 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. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

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.

7.1. Capacitaciones en Seguridad Digital

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. CUMPLIMINTO 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.

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 incluye lineamientos para el uso de equipos personales. Se incluye 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 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

Elaboró	Revisó	Aprobó
Catherine Suarez Rodríguez, Profesional de Seguridad de la Información -AND	Adriana Garces Ruíz Subdirectora Desarrollo y SCD William Roberto Pinzón Amézquita Planeación, Contratista	TORRES MOYA FIDEL ANTONIO Firmado digitalmente por TORRES MOYA FIDEL ANTONIO Fecha: 2025.02.25 15:49:36 -05'00' Fidel Antonio Torres Moya Director General