CONTENIDO

Proceso: Gestión de TI
POLÍTICA DE SEGURIDAD y PRIVACIDAD DE LA INFORMACIÓN
Versión: 2

1. OBJETIVO

Definir los lineamientos para preservar la integridad, disponibilidad y confidencialidad de la información de la Agencia Nacional Digital, a través del Sistema de Gestión de Seguridad de la (SGSI–PDP), implementando acciones de aseguramiento, conforme al cumplimiento de los requisitos legales, estratégicos, operativos, tecnológicos y tácticos, aplicando las buenas prácticas de seguridad de la información fundamentadas en la Norma ISO-IEC 27001:2013, en el contexto de direccionamiento estratégico y gestión del riesgo de la Agencia Nacional Digital.

2. ALCANCE

Aplica a todos los procesos, áreas y/o dependencias de la Agencia Nacional Digital, así como a todo el personal interno y externo de la Agencia Nacional Digital.

Las presentes políticas aplican para todos los activos de información que hacen parte de la Agencia Nacional Digital, de acuerdo con lo establecido en el *alcance del sistema de gestión de seguridad de la información y privacidad de los datos personales*.

Todos los directivos, Empleados de Planta, Contratistas, proveedores y Terceros que presten sus servicios o tengan alguna relación con la Agencia Nacional Digital deben dar cumplimiento a las políticas, en particular el personal que:

- Asuma roles de responsables o encargados de los datos personales.
- Acceda a información de la Agencia Nacional Digital.
- Opere equipos de cómputo, servidores, bases de datos, servicios y demás componentes tecnológicos, de seguridad y/o de comunicaciones de la Agencia Nacional Digital.
- Diseñe, construya, pruebe y/o utilice soluciones de software, sistemas de información, bases de datos o servicios colaborativos de la Agencia Nacional Digital.
- Provea servicios de gestión de información o de Información y tecnología.
- Acceda de manera física o lógica a las instalaciones de la Agencia Nacional Digital.
- Responsables y custodios de activos de información de la Agencia Nacional Digital.

3. DEFINICIONES

Con el propósito de facilitar la comprensión de la Política se deben tener en cuenta las siguientes definiciones:

3.1 Términos asociados a Seguridad de la Información:

a) Acceso privilegiado: Acceso dado a usuarios autorizados para el manejo de cuentas especiales relacionadas con sistemas críticos, bases de datos, redes de comunicaciones y herramientas de seguridad de la información.

b) Activo de Información: Todo lo que tiene valor para la Agencia Nacional Digital y que contiene, genera, procesa, almacena y le da un tratamiento a la información o se relaciona con la misma. Existen diferentes tipos de activos como: Información (bases de datos, bases de conocimiento), tecnológicos o digitales (hardware y software), infraestructura física (instalaciones, oficinas), organizacionales (procesos, metodologías, servicios) y el recurso humano (Empleados de Planta, Contratistas, proveedores, Terceros).

c) Activo Tecnológico: Son elementos físicos y lógicos que hacen parte de la infraestructura tecnológica (hardware y software), y redes de comunicaciones.

d) Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a los activos de información de la Agencia Nacional Digital.

e) Amenaza informática: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

f) Análisis de riesgos: Proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de éstas, a fin de determinar los controles adecuados para tratar el riesgo.

g) Ataques cibernéticos: Son ataques que tienen motivaciones económicas, sociales o políticas y se llevan a cabo a través de Internet, son dirigidos al público en general, a organizaciones privadas o países.

h) Autenticación: Permite establecer la validez de la información reconociendo la fuente y medio de verificación.

i) Autenticidad: Capacidad de demostrar la identidad del emisor con el objetivo de certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

j) Base de Datos: Se entiende como el conjunto organizado de datos de la Agencia Nacional Digital y de datos personales que sea objeto de Tratamiento.

k) Ciberamenaza: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste. (Glosario de Términos (CCN-STIC 401)).

l) Ciberdefensa: Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (Ej. Redes de computadoras, computadoras, programas informáticos, etc.), y cuyo campo de batalla es el Ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada Ciberguerra. (Glosario de Términos (CCN-STIC 401)).

m) Ciberespacio: Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos. Los sistemas interconectados en espacios aislados no forman parte del ciberespacio. (Glosario de Términos (CCN-STIC 401)).

n) Ciberincidente: Incidente relacionado con la seguridad de las TIC que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc. (Glosario de Términos (CCN-STIC 401)).

o) Ciberseguridad: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. (Glosario de Términos (CCN-STIC 401)).

p) COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

q) Confidencialidad: Atributo de la información que determina quién está autorizado a acceder a ella y previene su divulgación no autorizada dentro o fuera de la Agencia Nacional Digital.

r) Contraseña Fuerte: Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.

s) Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

t) Copias de Seguridad: Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla en caso de que ocurra un fallo que afecte a ésta y pueda estar disponible.

u) Custodio de activo de información: Parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad, de un activo de información.

v) Datos abiertos: 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 de 2014. Literal J, artículo 6. Definiciones).

w) Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. (Reglamento (UE) 2016/679 del parlamento europeo y del consejo).

x) Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012. Literal C, artículo 3. Definiciones).

y) Datos 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 1074 de 2015. Numeral 3, artículo 2.2.2.25.1.3. Definiciones).

z) Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1266 de 2008. Literal h), artículo 3. Definiciones).

aa) Dato público: 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 riesgos públicos, documentos públicos, gaceta y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva (Decreto 1074 de 2015. Numeral 2, artículo 2.2.2.25.1.3. Definiciones).

bb) Dato semiprivado: Es semiprivado el dato que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o grupo de

personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios (Ley 1266 de 2008. Literal g), artículo 3. Definiciones).

cc) Disponibilidad: Atributo de la información que determina para quién está disponible y los permisos de su uso dentro de las gestiones que adelante en la Agencia Nacional Digital.

dd) Encargado del Tratamiento: Es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos por cuenta del Responsable del Tratamiento (Ley 1581 de 2012. Literal D, artículo 3. Definiciones).

ee) Evento de seguridad de la información: Actividad sospechosa de un sistema, servicio o red, que indica una posible violación o falla de seguridad de la información, la cual requiere ser reportada de acuerdo con el *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la información* para ser analizada, resuelta y documentada por la Agencia Nacional Digital.

ff) Gestión de claves: son controles que se realizan mediante la gestión de claves criptográficas.

gg) Gestión de incidentes de seguridad de la información: Son las acciones de control para garantizar la seguridad de los activos de información y su apropiada gestión, implementando las acciones para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información en la Agencia Nacional Digital.

hh) Gestión de riesgos: Son las acciones que realiza la Agencia Nacional Digital para la identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

ii) Grupo de interés especial: Es un conjunto de personas, organizadas en torno a un interés común, con el fin de actuar conjuntamente en defensa del mismo.

jj) Hacking ético: Análisis de los sistemas y programas informáticos de la Agencia Nacional Digital, con el rol de un atacante y realizando ataques con el objetivo de evaluar el estado de seguridad de la información.

kk) Impacto: El costo para la organización de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. Consecuencia que sobre un activo tiene la materialización de una amenaza. [Magerit:2012].

ll) Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete la operación de la Agencia Nacional Digital.

mm) Incidente de bajo impacto: Este tipo de incidente afecta a activos de información considerados con una clasificación de bajo y/o menor impacto para la Agencia Nacional Digital, que no influyen en el cumplimiento de algún objetivo de los procesos de la Agencia Nacional Digital.

nn) Incidente medio impacto: Este tipo de incidente afecta a activos de información considerados con clasificación de impacto medio o moderado, que influyen directamente en los objetivos de los procesos de la Agencia Nacional Digital, su detección debe ocasionar un plan de mejoramiento de aplicación inmediata para superarlo.

oo) Información: Es un activo de valor que hace parte de la Agencia Nacional Digital, por la cual asume funciones como dueño o custodio de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la Entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de Terceros con los cuales dispone de un contrato, acuerdo o convenio; y datos personales de los cuales asume un rol como responsable o encargada de los mismos.

pp) Incidente de alto impacto: Este tipo de incidente afecta a activos de información considerados con clasificación de impacto alto o crítico para la Agencia Nacional Digital, que influyen directamente a los objetivos misionales de la Agencia Nacional Digital. Esta categoría de incidentes afecta la reputación y el buen nombre de la Entidad y pueden involucrar aspectos legales. Para estos incidentes la respuesta debe ser inmediata y desencadenar un plan de choque en el marco de las acciones y estrategias de continuidad del negocio.

qq) Integridad: Atributo de la información que protege los activos de información sobre posibles alteraciones, modificaciones no autorizadas formalmente por la Agencia Nacional Digital.

rr) Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la Agencia Nacional Digital y necesiten por tanto ser protegidos de potenciales riesgos.

ss) Matriz de Vulnerabilidades: Documento que permite hacer recopilación de las vulnerabilidades identificadas y detectadas en la Agencia Nacional Digital.

tt) No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron. [UNE-ISO/IEC 27000:2014].

uu) Parches de seguridad: Son los cambios que se aplican al software para corregir vulnerabilidades.

vv) Parte interesada (Stakeholder): persona u organización (usuarios directos e indirectos, entidades públicas, Terceros relacionados, entidades externas) que puede afectar, ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

ww) Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

xx) Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implementar los controles necesarios para proteger la misma.

yy) Principios de Seguridad de la Información: son características propias de la protección de la información: la Confidencialidad, Integridad y Disponibilidad.

zz) Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

aaa) Responsable de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

bbb) Riesgo: Es la probabilidad de que una amenaza o vulnerabilidad pueda ocasionar la pérdida y/o alteración de la información de la Agencia Nacional Digital.

ccc) Responsable del tratamiento: persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos (Ley 1581 de 2012. Literal E, artículo 3. Definiciones). Para efectos de esta Política, el Responsable del Tratamiento es la Agencia Nacional Digital.

ddd) Segregación de tareas: Procedimiento de seguridad que exige la concurrencia de dos o más personas para realizar tareas críticas. De este modo, se anula la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita. (Glosario de Términos (CCN-STIC 401)).

eee) 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. (CONPES 3854 Política Nacional de Seguridad Digital).

fff) Seguridad Informática: preservación de la información que se genera, procesa, almacena o transmite a través de un entorno tecnológico.

ggg) Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

hhh) Servicios Ciudadanos Digitales: Son un conjunto de soluciones tecnológicas que buscan facilitar a los usuarios, y en específico a los ciudadanos, su interacción con las entidades públicas y optimizar la labor del Estado.

iii) Sistema de Gestión de Seguridad de la Información (SGSI): Es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implementación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información. (Glosario de términos de ciberseguridad de INCIBE).

jjj) Titular de la información: Persona natural cuyos datos personales sean objeto de tratamiento (Ley 1581 de 2012. Literal F, artículo 3. Definiciones).

kkk) Teletrabajo: actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo, contemplando un entorno físico y/o virtual.

lll) Trabajo remoto: Es el trabajo realizado a distancia utilizando las TICs para producir bienes y servicios por cuenta propia o ajena.

mmm) Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

nnn) Vulnerabilidad: Es la debilidad o fallo del sistema que pone en riesgo la confidencialidad, integridad y disponibilidad de la información de la Agencia Nacional Digital.

ooo) VPN (Virtual Private Network): Es una tecnología que permite establecer una red privada que cifra el tráfico que viaja y permite mantener la confidencialidad e integridad dificultando que un tercero pueda robar información.

3.2 Términos asociados a Documentación y procesos administrativos

ppp) Contratista: Persona natural o jurídica contratada por la Agencia Nacional Digital para la adquisición de una obra, bien o servicio, no perteneciente al régimen laboral.

qqq) Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la Agencia Nacional Digital antes de crear nuevas políticas[1].

rrr) Política: Declaración de alto nivel que describe la posición de la Agencia Nacional Digital sobre un tema específico[2].

sss) Procedimiento: Documento que define los pasos a seguir y que deben ser implementados en una situación dada.

ttt) Proveedor: Persona natural o jurídica contratada para proveer a la Agencia Nacional Digital de un producto o servicio.

uuu) Trabajador: Persona natural que presta un servicio personal a la Agencia Nacional Digital bajo la continuada dependencia o subordinación y mediante remuneración.

4. DOCUMENTOS DE REFERENCIA

- **Ley 23 de 1982**, por la cual se regulan los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita.

- **Ley 597 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, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 594 de 2000**. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

[1] Tomado del Glosario de http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf
[2] Tomado del Glosario de http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- **Ley 1266 de 2008**, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de Terceros países.

- **Ley 1273 de 2009**, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- **Ley 1581 de 2012**, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

- **L**ey 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Documento CONPES 3854**, Política Nacional de Seguridad Digital.

- **ISO 27001:2013**, es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Los Sistemas Gestión de la Seguridad de la Información permiten a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

- **ISO 27035:2012,** enfoque de mejores prácticas destinado a la gestión de la información de incidentes de seguridad.

- **ISO 22301:2012,** norma que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un Sistema de Gestión de la Continuidad del Negocio.

- **NIST framework Ciberseguridad**, es el marco que permite a las organizaciones comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1. Definición de la Política

La Agencia Nacional Digital como articulador y prestador de los Servicios Ciudadanos Digitales y del sistema de planeación y gestión pública, y desarrollar las actividades de ciencia, tecnología e innovación

asociadas a la creación de un ecosistema de información pública, incorporando la debida gestión de riesgos asociada a la información, que permita apoyar proyectos de ciencia, tecnología e innovación, así como identificar planes, programas y proyectos que ofrezcan soluciones a problemáticas o cuellos de botella en el sector público colombiano, introduciendo con ello mejoras significativas en los procesos estatales, mediante el uso y desarrollo de soluciones de software, analítica de datos, entre otras desarrollador de soluciones de software que apoyan y facilitan los procesos de las Entidades Públicas, entendiendo la importancia fundamental de la información y los datos personales para el desarrollo de su objeto y la toma de decisiones adecuadas y eficientes, tiene como compromiso la protección y salvaguarda de ésta preservando su confidencialidad, integridad y disponibilidad, con base en la administración de riesgos, la continuidad de las operaciones y logrando una cultura y conciencia organizacional de seguridad y privacidad de la información.

Por medio de la presente Política, la Agencia Nacional Digital busca establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes, buenas prácticas y en concordancia con la misión y visión de la Entidad, para obtener un nivel de exposición que permita dar cumplimiento a los criterios de prestación de los servicios y lo establecido en seguridad y privacidad de la información.

5.1.1. Orientación de la Dirección para la Gestión de la Seguridad y Privacidad de la Información

La Agencia Nacional Digital, con el compromiso de la Alta Dirección, ha establecido los lineamientos pertinentes en cada Componente de Seguridad y Privacidad de la Información, de acuerdo con los principios de confidencialidad, integridad y disponibilidad; y la administración del riesgo sobre los que se basa el desarrollo de las acciones, la toma de decisiones y la gestión de incidentes alrededor de un Sistema de Gestión de Seguridad de la información – SGSI. Dando cumplimiento a lo anterior, a continuación, se definen las políticas que se encuentran en el presente documento, para la operación y la relación con proveedores y Terceros de la Agencia Nacional Digital.

5.1.2. Revisión de las Políticas de Seguridad y Privacidad de la Información

Las políticas de seguridad y privacidad de la información deben ser revisadas por la Alta Dirección, Control Interno, el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales de la Agencia Nacional Digital de manera anual o por demanda, cada vez que sea requerido, permitiendo la evaluación y mejora continua de las mismas.

6. ORGANIZACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. Organización Interna

La Agencia Nacional Digital ha establecido una estructura organizacional en torno al manejo de la seguridad y privacidad de la información. Así es como ha conformado el Equipo de Seguridad de la Información y Equipo de Protección de Datos Personales a nivel estratégico como parte de la Alta Dirección, dando direccionamiento y gestión como un eje transversal a toda la organización y operaciones.

6.1.1 Roles y Responsabilidades de Seguridad y Privacidad de la Información

Para llevar a buen término el cumplimiento de las políticas y gestión de la seguridad y privacidad de la información se han establecido los siguientes roles y responsabilidades en la Agencia Nacional Digital:

Alta Dirección

La Alta Dirección, conformada a través del Comité de Gestión y Desempeño o quien haga sus veces, es la encargada de definir estrategias, tomar decisiones, aprobar los recursos necesarios, determinar el nivel de riesgo de aceptación residual y la clasificación de los activos de información, y hacer seguimiento anualmente o cuando se requiera a las políticas y el Sistema de Gestión de Seguridad de la Información.

Comité de Seguridad y Privacidad de la Información o quien haga sus veces:

Este comité es conformado por la Dirección, la Subdirección de Servicios Ciudadanos Digitales, la Subdirección de Desarrollo, la Subdirección Administrativa y Financiera y la Subdirección Jurídica, Control Interno, Gestión de Tecnologías de la Información, Oficial de Privacidad de la Información, Oficial de Seguridad de la Información y los demás actores responsables que pueden interactuar en el proceso .

Las responsabilidades de este Comité son las siguientes:

- Establecer estrategias que permitan el mejoramiento de la seguridad y privacidad de la información en la Agencia Nacional Digital.
- Revisar y aprobar las políticas, procedimientos, metodologías, formatos y demás elementos del Sistema de Gestión de Seguridad de la Información.
- Revisar la gestión de seguridad y privacidad de la información en términos del cumplimiento de las políticas establecidas en este documento y la normativa legal vigente.
- Tomar decisiones sobre los incidentes de seguridad y continuidad de las operaciones en términos de la afectación de misión y visión de la Agencia Nacional Digital.

- Gestionar recursos con la Alta Dirección para el cumplimiento de la gestión de la seguridad y privacidad de la información.
- Validar el cumplimiento de los requisitos legales, contractuales, normativos y buenas prácticas de seguridad y privacidad de la información.

El Oficial de Seguridad de la Información

Es el encargado de liderar, planear, coordinar, revisar, hacer seguimiento y control al cumplimiento de las políticas, gestión de riesgos, definición de controles que permitan la mejora continua de la seguridad de la información de la Agencia Nacional Digital. Así mismo, debe reportar o informar de la gestión de la seguridad de la información a la Alta Dirección. Así mismo, cualquier excepción a lo establecido en esta política, debe contar con la aprobación formal del Comité de Seguridad y Privacidad de la Información o quien haga sus veces.

Debe interactuar directamente con el Oficial de Protección de Datos Personales en términos de direccionar y coordinar la seguridad de los datos personales fundamentados en el cumplimiento de los requisitos legales y de las buenas prácticas de seguridad de la información establecidas.

Profesional de Seguridad de la Información

Debe apoyar la gestión, definición, implementación, mantenimiento y cumplimiento de las políticas y gestión de riesgos de seguridad de la información en conjunto con el Oficial de Seguridad de la Información. Así mismo, realizar actividades administrativas y técnicas requeridas para llevar al cumplimiento de éstas.

Control Interno

Debe realizar el respectivo seguimiento al cumplimiento de las políticas y al Sistema de Gestión de Seguridad de la Información conforme a los requisitos legales, normativos y técnicos establecidos por la Agencia Nacional Digital. Así mismo, se encarga de notificar al Oficial de Seguridad de la Información, al Oficial de Protección de Datos Personales y a este Comité los hallazgos y acciones para el mejoramiento de la seguridad y privacidad de la información.

Gestión de Tecnologías de la Información

Debe apoyar el cumplimiento de las políticas y gestión de la seguridad y privacidad de la información mediante la implementación, configuración y monitoreo de las herramientas tecnológicas, redes y

seguridad necesarias para el control, manejo, transporte, almacenamiento y procesamiento seguro de la información. Así mismo, debe apoyar la gestión de los incidentes tecnológicos y la continuidad de las operaciones de la Agencia Nacional Digital.

Líderes de Proceso

Deben cumplir las políticas de seguridad y privacidad de la información y velar por el cumplimiento de las mismas en sus equipos de trabajo, aplicar las medidas necesarias para la protección de los activos de información que le han sido asignados. Así mismo, es su deber fomentar y hacer seguimiento mínimo una vez al mes, o cuando sea requerido, al cumplimiento de las políticas de seguridad y privacidad de la información.

Debe apoyar la gestión de riesgos de seguridad y privacidad de la información conforme a la *Política y metodología de gestión de riesgos* establecida por la Agencia Nacional Digital.
Es responsable de informar al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales cualquier evento o riesgo materializado o posible materialización.

Oficial de Protección de Datos Personales

Encargado de liderar, planear, coordinar, revisar, hacer seguimiento y control al cumplimiento efectivo de las políticas, procedimientos, gestión de riesgos, definición de controles que permitan la protección de los datos personales administrados por la Agencia Nacional Digital. Así mismo, debe reportar o informar de la gestión para la protección de los datos personales a la Alta Dirección. Así mismo, cualquier excepción a lo establecido en esta política, debe contar con la aprobación formal del Comité de Seguridad y Privacidad de la Información.

Debe interactuar directamente con el Oficial de Seguridad de la Información en términos de direccionar y coordinar la seguridad de los datos personales fundamentados en el cumplimiento de los requisitos legales y de las buenas prácticas de seguridad de la información establecidas.

Empleados de Planta en General de la Agencia Nacional Digital

Todos los Empleados de Planta de la Agencia Nacional Digital son responsables de cumplir y hacer buen uso de las políticas de seguridad y privacidad de la información en el desarrollo de todas sus funciones. Así mismo, son responsables de reportar o informar oportunamente al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales cualquier incidente o riesgo identificado sobre la información y datos personales.

Contratistas, Proveedores y Terceros

Toda persona que tenga una relación jurídica (a través de un acuerdo, contrato o convenio) con la Agencia Nacional Digital debe cumplir con las políticas de seguridad y privacidad de la información y cláusulas establecidas en el documento que regule la relación jurídica. Así mismo, son responsables de reportar o informar oportunamente al Supervisor del acuerdo, contrato o convenio los riesgos, incidentes o cualquier evento que pueda poner en riesgo la seguridad y privacidad de la información durante la prestación de sus servicios o durante la relación jurídica.

6.1.2 Segregación de Funciones

Las funciones o actividades en materia de seguridad y privacidad de la información en la Agencia Nacional Digital son definidas por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con el apoyo del Proceso de Gestión de Talento Humano, para Empleados de Planta, y contratistas, con el visto bueno del Comité de Gestión y Desempeño quién a su vez apoya la oficialización de las mismas a través del *Manual de Funciones* y los Contratos de Prestación de Servicios.

Las funciones o actividades de seguridad y privacidad de la información deben ser asignadas a roles y talento humano que disponga con las competencias pertinentes para desarrollarlas de acuerdo con el *procedimiento de selección de personal* y al *procedimiento de gestión contractual* establecidos.

Las funciones o actividades relacionadas con seguridad y privacidad de la información para todos los Empleados de Planta y contratistas de la Agencia Nacional Digital deben estar orientadas por: políticas y lineamientos de seguridad y privacidad de la información, los procesos y ser reflejadas en los contratos de los Empleados de Planta y contratistas que hacen parte de la Agencia Nacional Digital, conforme a su rol y responsabilidad sobre los activos de información.

Todo Empleado de Planta, Contratista o Tercero está en la facultad de acceder y utilizar la información de la Agencia Nacional Digital conforme a las disposiciones constitucionales y legales; y a las autorizaciones previas por parte de los propietarios o responsables de la misma.

Todos los Procesos son responsables del control y tratamiento de la información en su área. Por tal motivo, es su deber velar por el cumplimiento de las políticas de seguridad y privacidad de la información, la actualización, reporte y cumplimiento de los controles establecidos por la entidad para proteger la información.

6.1.3 Contacto con las Autoridades

La Agencia Nacional Digital, como parte del aseguramiento de los activos de información, debe establecer y mantener un contacto con las autoridades legales, autoridades civiles y militares propias de la materia, organismos de control para el caso de incidentes que conllevan al incumplimiento de la legislación y normativas internas propias de la entidad. Para casos de incidentes de seguridad que afecten a Terceros, se deben adelantar las acciones correspondientes que procedan a la investigación pertinente de las autoridades.

Para el caso de ataques o delitos cibernéticos identificados, la Agencia Nacional Digital debe informar a las autoridades competentes para que se adelanten las acciones correspondientes.

Para asegurar la continuidad de las operaciones, la Agencia Nacional Digital, de acuerdo con el plan de continuidad del negocio, debe definir, establecer y mantener actualizados los contactos necesarios con las autoridades y empresas de servicios públicos (energía, agua, seguridad, comunicaciones), servicios de emergencia, departamentos de bomberos. Así mismo, debe mantener sus contactos actualizados en materia de telecomunicaciones con los operadores que actualmente prestan este servicio y los demás que se requieran.

6.1.4 Contacto con los Grupos Especiales

La Agencia Nacional Digital, en virtud de permanecer actualizada frente al manejo de la seguridad y privacidad de la información, debe mantener un contacto con grupos especialistas en la materia. De esta manera, debe establecer alianzas estratégicas con organizaciones, foros y/o eventos que permitan adquirir, fortalecer y fomentar el conocimiento de las mejores prácticas de seguridad y privacidad de la información, alertas oportunas o tempranas de riesgos o incidentes de seguridad, resolución de incidentes, asesorías especializadas, tecnologías de punta en seguridad, amenazas y vulnerabilidades informáticas actuales.

En caso de compartir información con grupos de interés especial, se debe contar con un procedimiento que establezca los controles para hacerlo de manera segura y confiable y que sea propio del beneficio de la Agencia Nacional Digital y grupos vinculados por el fin común de mejoramiento a las buenas prácticas de seguridad y privacidad de la información en las entidades públicas o privadas. Dicho intercambio debe evaluarse frente a los riesgos y debe ser autorizado por el Comité de Seguridad y Privacidad de la Información. Así mismo, en el caso del Servicio Ciudadano Digital de Interoperabilidad que presta la

Agencia Nacional Digital, en el cual se le provee solo la plataforma para el intercambio de información, dichos acuerdos de intercambio de información son responsabilidad de los terceros responsables.

6.1.5 Seguridad y Privacidad de la Información en la Gestión de Proyectos

La Agencia Nacional Digital debe contar con una metodología documentada de Gestión de Proyectos, que incluya en cada una de sus fases los controles de seguridad, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información.

Todos los proyectos de la Agencia Nacional Digital internos o externos deben incorporar requisitos de seguridad de la información, protección de los datos personales y gestión de riesgos sobre los mismos.

Los requisitos de seguridad y privacidad de la información de todo proyecto deben ser definidos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, respectivamente; y aceptados y acogidos por los Gerentes de Proyecto, quien a su vez se debe encargar de hacerlos efectivos dentro de cada proyecto que se lleve a cabo.

Todo proyecto de la Agencia Nacional Digital debe incorporar objetivos de seguridad y valoración de riesgos.

Los Gerentes de Proyecto son responsable del cumplimiento de los requisitos de seguridad y privacidad de la información en los proyectos. Por tanto, debe revisar periódicamente dicho cumplimiento a través de los seguimientos establecidos en el desarrollo de los proyectos. Este seguimiento debe ser registrado a través de actas de reuniones de seguimiento del proyecto o como se defina y establezca dentro de la metodología.

Cualquier incumplimiento de los requisitos de seguridad y privacidad de la información establecidos para los proyectos deben ser informados oportunamente por el Supervisor del Proyecto al Gerente de Proyecto asignado; y así mismo los Gerentes de Proyecto debe informarlo al Oficial de Seguridad de la Información y/o al Oficial de Protección de Datos Personales, quien(es) a su vez debe(n) tomar las medidas pertinentes para gestionarlo.

El Supervisor del Proyecto debe reportar a los Gerentes de Proyectos, y este a su vez al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales los incidentes, eventos de seguridad, riesgos materializados del proyecto, con el fin de aplicar el *procedimiento de notificación y gestión de incidentes de seguridad de la información* y la *metodología de riesgos.*

6.2 Dispositivos Móviles y Teletrabajo o Trabajo Remoto

La Agencia Nacional Digital debe asegurar el uso de la información y protección de datos personales a través del Teletrabajo o trabajo remoto y uso de dispositivos móviles por parte de sus Empleados de Plantas, Contratistas o proveedores de servicios autorizados.

6.2.1. Lineamientos para Uso de Dispositivos Móviles

La Agencia Nacional Digital establece el uso de dispositivos móviles enfocado en el aseguramiento de la información a través de los siguientes lineamientos de control:

- El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, con el apoyo del Proceso de Gestión de Tecnologías de la Información, deben avalar la seguridad y privacidad de la información en los dispositivos móviles externos a la Agencia, que porten sus Empleados de Planta y contratistas, siempre y cuando se recolecte, administre, transmita, transfiera, almacene o procese información de la Agencia.
- Todo uso de dispositivos móviles para desarrollar las actividades o funciones de la Agencia Nacional Digital, debe ser evaluado previamente frente a sus riesgos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, y aprobado o autorizado por la Subdirección Administrativa y Financiera.
- En la Agencia Nacional Digital se debe permitir el uso de dispositivos móviles de la Entidad solo para desarrollar las funciones u actividades del contrato. Cualquier uso de dispositivos móviles diferentes a los de la Entidad debe ser evaluado frente a los riesgos por el Comité de Seguridad y Privacidad de la Información, quien a su vez debe aprobar o no su uso.
- Para el caso de dispositivos móviles privados o personales. Su uso deber ser autorizado por el Comité de Seguridad y Privacidad de la Información. Así mismo, debe establecerse un acuerdo con el Empleado de Planta o contratista en el que reconoce sus deberes frente a la protección física, control de acceso, actualización de software, copias de seguridad, tratamiento de datos personales, propiedad de la información, confidencialidad de la información, borrado seguro de la información al terminar el acuerdo y demás lineamientos establecidos en dicho acuerdo que permitan asegurar el uso de la información conforme a la normativa de protección de datos personales y normativas internas de la Agencia Nacional Digital.
- Los Empleados de Planta y contratistas que utilizan dispositivos móviles personales son responsables de informar oportunamente a su Jefe inmediato o Supervisor de Contrato cualquier incidente o riesgo en el cual se vea afectada la información de la Agencia Nacional Digital.
- Es responsabilidad de los Empleados de Planta y contratistas que utilizan dispositivos móviles acatar las medidas de seguridad y privacidad de la información pertinentes sobre su uso, como: evitar no utilizar la información o interacción de canales de la Agencia conectado a redes públicas.

- No descargar información de la Agencia Nacional Digital en otros dispositivos no autorizados, mantener su dispositivo con usuario y contraseñas seguras.
- Todo dispositivo móvil autorizado deber ser registrado de acuerdo con el *procedimiento de gestión de activos de información.*
- Todos los dispositivos móviles autorizados para uso de las operaciones deben estar protegidos a nivel físico. Para esto, la Agencia Nacional Digital debe suministrar los elementos de protección necesarios para los mismos, tales como: protectores, forros, maletines, guayas, entre otros, según sea el caso.
- Todo dispositivo móvil autorizado y suministrado por la Agencia Nacional Digital debe estar dotado del software de seguridad necesario para proteger la información.
- Toda instalación de servicios institucionales como correo electrónico, servidores de archivos, entre otros, en dispositivos móviles debe ser autorizado por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.
- El Proceso de Gestión de Tecnologías de la Información es el responsable de controlar a nivel tecnológico el uso de dispositivos Móviles. Para esto, es encargado de:

    - Controlar la instalación de software no autorizado en los dispositivos móviles, restringiendo dicha funcionalidad en los mismos.
    - Aplicar parches y cambiar las versiones del software a los dispositivos móviles a través del *procedimiento de gestión de cambios*.
    - Restringir la conexión a servicios de información no autorizada sobre los dispositivos móviles.
    - Establecer e implementar mecanismos de control de acceso sobre uso de los dispositivos móviles.
    - Implementar técnicas o mecanismos criptográficos propuestos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales para los dispositivos móviles.
    - Instalar herramientas de protección contra códigos maliciosos como antivirus, propuestos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.
    - Establecer e implementar mecanismos de control remoto sobre los dispositivos móviles.
    - Realizar copias de seguridad o respaldo de la información sobre los dispositivos móviles.
    - Configurar uso de servicios y aplicaciones web conforme a las autorizaciones dadas sobre los mismos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.

6.2.2. Trabajo remoto y/o teletrabajo

La Agencia Nacional Digital debe definir el proceso de implementación de trabajo remoto y/o teletrabajo, de acuerdo con la normativa y los lineamientos exigidos en este tema y en aras de salvaguardar la información.

La Agencia Nacional Digital debe preservar la seguridad y privacidad de la información frente a riesgos asociados al trabajo remoto y/o teletrabajo de acuerdo con los procedimientos definidos para tal fin.

Se deben implementar los siguientes lineamientos para un trabajo remoto y/o teletrabajo en condiciones óptimas de seguridad:

La Subdirección Administrativa y Financiera es la encargada de autorizar el uso de trabajo remoto y/o teletrabajo, conforme a la normatividad y los lineamientos establecidos en la Agencia Nacional Digital.

La Subdirección Administrativa y Financiera, con el apoyo del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, debe validar la seguridad física del sitio de trabajo remoto y/o teletrabajo y su entorno para ser viable su aprobación.

La Subdirección Administrativa y Financiera, con el apoyo del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, debe definir los entornos físicos y de seguridad y privacidad idóneos para ejercer el trabajo remoto y/o teletrabajo.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben definir los requisitos de seguridad de la información a nivel físico, lógico conforme a la necesidad de acceso remoto a los sistemas y a la información; el control de acceso, canales de comunicación y la sensibilidad de información que manejará el usuario.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, en apoyo con el Proceso de Gestión de Tecnologías de la Información, deben analizar la viabilidad de dotar de un entorno virtual para el uso de trabajo remoto y/o teletrabajo, de tal manera que se evite el uso de información de la Agencia en repositorios de equipos privados. Esto para el caso de autorización de equipos personales para uso de trabajo remoto y/o teletrabajo.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben emitir recomendaciones en el uso seguro de la información en ambientes de teletrabajo, considerando amenazas informáticas.

Se prohíbe el uso de redes públicas en entornos de trabajo remoto y/o teletrabajo.

En el caso de uso de redes domésticas para el trabajo remoto y/o teletrabajo se requiere que el usuario mantenga configuraciones adecuadas de seguridad como usuario y contraseñas seguras, software antimalware, entre otros, según lo establecido en esta Política.

El usuario de trabajo remoto y/o teletrabajo es responsable del uso de la información conforme a los derechos de autor y propiedad intelectual, reconociendo que la Agencia Nacional Digital es propietaria de la información que le ha suministrado para el desarrollo de actividades laborales, o de terceros que contrataron a la Agencia Nacional Digital para la prestación de un servicio.

El usuario debe hacer buen uso de la información, resultado del desempeño de sus actividades laborales o contractuales. El uso indebido es motivo de sanción o penalización conforme a la ley y a las políticas de seguridad y privacidad de la información de la Agencia Nacional Digital.

En el caso de dotación de equipos de la Entidad para trabajo remoto y/o teletrabajo, la Agencia Nacional Digital debe dotar de las licencias de software necesario para el desarrollo de las funciones laborales o contractuales. En el caso de equipos personales autorizados para trabajo remoto y/o teletrabajo la Agencia Nacional Digital debe suministrar el licenciamiento de software contenido en un entorno virtual propio de la entidad, dejando bajo la responsabilidad del usuario el software utilizado a nivel personal del mismo. Para esto, se debe establecer un acuerdo de licenciamiento entre la Agencia Nacional Digital y el usuario de trabajo remoto y/o teletrabajo.

La Agencia Nacional Digital, a través del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, con el apoyo del Proceso de Gestión de Tecnologías de la Información, debe implementar los requisitos técnicos de seguridad y privacidad de la información para uso de trabajo remoto y/o teletrabajo, tales como: Firewall, Antimalware, aseguramiento de los equipos, entre otros.

La Subdirección Administrativa y Financiera se encarga de suministrar el equipo y elementos adecuados para las actividades de trabajo remoto y/o teletrabajo, esto cuando se establece el uso de equipos de la Agencia.

La Subdirección Administrativa y Financiera debe establecer los horarios de trabajo permitidos para los Empleados de Planta de trabajo remoto y/o teletrabajo, con el fin de coordinar con el Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y el Proceso de Gestión de Tecnologías de la Información, la clasificación de la información, los sistemas, servicios e información de la que puede disponer durante sus labores o actividades.

La Subdirección Administrativa y Financiera, con el apoyo del Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y el Proceso de Gestión de Tecnologías de la Información, debe

suministrar los dispositivos tecnológicos y el software necesarios para llevar a cabo el trabajo remoto y/o teletrabajo de manera eficiente.

El Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y la Subdirección Administrativa y Financiera deben determinar los lineamientos de seguridad de la información necesarios para el trabajo remoto y/o teletrabajo, incluyendo recomendaciones relacionadas con el control de acceso a la información y de personal no autorizado (familiares o visitantes).

El Proceso de Gestión de Tecnologías de la Información es responsable de suministrar soporte y mantenimiento del hardware y software para el desarrollo del trabajo remoto y/o teletrabajo. Esto aplica para dispositivos suministrados por la Entidad. En el caso de dispositivos personales previamente aprobados para su uso por la Agencia Nacional Digital, es responsabilidad del usuario el soporte y mantenimiento del software y hardware.

La Subdirección Administrativa y Financiera debe suministrar las pólizas de seguro sobre los dispositivos de la Entidad asignados a trabajo remoto y/o teletrabajo.

El Proceso de Gestión de Tecnologías de la Información con su equipo de trabajo es responsable de realizar las copias de seguridad de los equipos asignados a trabajo remoto y/o teletrabajo conforme al *procedimiento de copias de seguridad de la información* de la Agencia Nacional Digital.

El Proceso de Gestión de Tecnologías de la Información es responsable de mantener la disponibilidad de la operación del trabajo remoto y/o teletrabajo considerando un alcance relacionado exclusivamente con los recursos dispuestos por la Agencia Nacional Digital. Aquellos recursos utilizados por los usuarios que no hacen parte de la Agencia Nacional Digital, tales como, dispositivos personales, redes de internet domésticas, entre otros, no se contemplan en este alcance, asumiendo la responsabilidad el usuario sobre los mismos para su propia continuidad de la labor o prestación.

La Agencia Nacional Digital se reserva el derecho de revocación de la autoridad y derechos de acceso sobre los activos de información proporcionados para el trabajo remoto y/o teletrabajo. En tal caso, es deber del usuario devolver los activos asignados, conforme al *procedimiento de devolución de activos de información*.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

7.1. Antes de Asumir el Empleo

La Agencia Nacional Digital debe implementar los controles necesarios, con el fin de que el personal que se contratado (Empleados de Planta y Contratistas) para identificar que son idóneos el desarrollo de las laborales para los cuales han sido o van hacer contratados.

7.1.1. Selección del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo, cual incluyan los aspectos legales y de procedimiento que dicta el proceso de contratación de Empleados de Planta y Contratistas de la Agencia Nacional Digital.

Se debe definir y establecer los procedimientos de selección, vinculación y desvinculación de personal, en los cuales se incluyen los controles de seguridad y privacidad de la información.

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación vigente y que aplique.

Acuerdo de Confidencialidad

Todos los Empleados de Planta, Contratistas y Terceros que ingresen a trabajar a la Agencia Nacional Digital, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios, contrato de planta, acta de posesión del Empleado de Planta. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el Proceso de Gestión de Talento Humano y Contractual, según sea el caso y aplique.

Dentro del mismo acuerdo el Empleado de Planta, Contratista o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Empleado de Planta, Contratista o Tercero.

7.1.2. Términos y Condiciones del Empleo

Antes de contratar al personal se deben establecer los términos y condiciones del empleo, las responsabilidades propias de sus funciones, de seguridad Y privacidad de la información para Empleados de Planta y Contratistas el cual es formalizado a través del contrato laboral.

Todos los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte de los contratos o documentos de vinculación que sean establecidos.

Todos los Empleados de Planta, Contratistas y Terceros, durante el proceso de vinculación a la Agencia Nacional Digital, deben recibir una inducción sobre las Políticas de Seguridad y Privacidad de la Información.

7.2. Durante la Ejecución del Empleo

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con el apoyo de la Subdirección Administrativa y Financiera son los encargados de asegurarse que los Empleados de Planta y Contratistas conozcan y mantengan una conciencia y cumplan las responsabilidades de seguridad y privacidad de la información.

7.2.1. Responsabilidades de la Dirección

Es deber de la Dirección, Subdirecciones y Líderes de Proceso deben exigir a los Empleados de Planta y Contratistas el cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información. Para esto, debe incorporar esta temática en su seguimiento y control de actividades propias de su área.

7.2.2. Toma de Conciencia, Educación y Formación en Seguridad y Privacidad de la información

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con el apoyo de la Subdirección Administrativa y Financiera se deben definir, coordinar actividades periódicas mínimo una vez al año sobre capacitaciones en seguridad y privacidad de la información, con el fin de fomentar y mantener una cultura organizacional sobre el cumplimiento de las políticas y procedimientos de seguridad de la información y privacidad de los datos personales. Así mismo, de manera extemporánea pueden realizar actividades de sensibilización cuando sea requerido a través de los canales de comunicación de la Agencia Nacional Digital.

7.2.3. Proceso Disciplinario

La Agencia Nacional Digital debe establecer un control disciplinario comunicado a todos los Empleados de Planta, Contratistas y Terceros en el cual se determinan el deber proceder de la Agencia frente a posibles incumplimientos o violaciones a la seguridad y privacidad de la información.

Todos los incidentes de seguridad de la información presentados en la Agencia Nacional Digital, deben tener el tratamiento adecuado, según lo establecido en el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*, con el fin de determinar sus causas y responsables, teniendo en cuenta el impacto y las responsabilidades identificadas para tomar acciones y se realizar el respectivo traslado ante las instancias correspondientes.

En lo pertinente al incumplimiento de las políticas de seguridad de la información de la Entidad, a los Empleados de Planta, Contratistas y Terceros, se les debe aplicar lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

7.3. Terminación y Cambio de Empleo

La Agencia Nacional Digital debe establecer los controles necesarios para la protección de los intereses de la Entidad, frente a la terminación o cambio de roles o funciones en contratos de Empleados de Planta, Contratistas y Terceros. Para esto, la Subdirección Administrativa y Financiera define y aplica cláusulas contractuales que permitan proteger la seguridad y privacidad de la información conforme a lo establecido en el *procedimiento de contratación* de la Agencia.

7.3.1. Responsabilidades en la Terminación o Cambio del Empleo

La Subdirección Administrativa y Financiera una vez identifique o determine una terminación o cambio en el contrato de Empleados de Planta o Contratistas debe informar a los mismos sus responsabilidades y deberes sobre la seguridad y privacidad de la información.

8. GESTIÓN DE ACTIVOS

En la Agencia Nacional Digital se gestionan los activos de información conforme a las políticas y procedimientos establecidos.

Se debe definir y establecer un documento de Gestión de Activos de Información, en el cual se detalle como se va a realizar el levantamiento, como se va a evaluar cada activo y con que criterios, roles y responsabilidades y mejora continua de esta actividad.

8.1. Responsabilidad por los Activos de Información

Todos los activos de información deben tener un responsable, que garantice la protección de la información y los datos que son almacenados en cada uno de los activos.

Todos los responsables de los activos de información deben hacer buen uso de los mismos y garantizar la integridad, disponibilidad confidencialidad de los mismos.

8.1.1. Inventario de Activos

Cada Proceso en la Agencia Nacional Digital, con el apoyo del Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y Gestión Documental es responsable de identificar y registrar en la matriz definida los activos de su proceso.

8.1.2. Propiedad de los Activos

Todo activo de información debe tener un propietario, quién se encarga de velar por el buen uso y cumplimiento de las políticas de seguridad y privacidad de la información.

8.1.3. Uso aceptable de activos de información

La Agencia Nacional Digital define los lineamientos para el uso aceptable de los activos de información.

Obligaciones:

1. Los activos de información solamente pueden ser utilizados con fines laborales y que se encuentren relacionados directamente con las funciones laborales y objeto contractual.

2. Cada activo de información tiene designado un propietario en el inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información de este.

3. El uso de activos fuera de las instalaciones debe tener el permiso escrito previo del jefe del área encargada y deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

4. Todos los Empleados de Planta, Contratistas y Terceros deben hacer la devolución de todos activos a su cargo cuando finalice el contrato laboral.

5. Todos los Empleados de Planta, Contratistas y Terceros deben realizar copia de seguridad de toda la información clasificada como confidencial, sensible, reservada o reservada clasificada que se encuentra almacenada en el equipo que tiene asignado.

6. Todos los equipos de cómputo deben tener instalado el software antimalware y de seguridad que provee la Agencia Nacional y debe contar con la opción de actualización automática activada.

7. Todos los Empleados de Planta, Contratistas y Terceros solamente pueden acceder a los activos de información, previa autorización del propietario del activo y en cumplimiento a los procedimientos establecidos de acceso a la información.

8. Todos los Empleados de Planta, Contratistas y Terceros que realicen actividades para la Agencia Nacional Digital solo deben acceder a la información necesaria para el desempeño de las actividades o funciones laborales.

9. Todos los Empleados de Planta de la Agencia Nacional Digital deben reportar sin demoras injustificadas a los responsables de sus áreas, al Oficial de Seguridad de la información y al Oficial de Protección de Datos Personales, cualquier evento o incidente que pueda afectar la integridad, disponibilidad, confidencialidad o privacidad de cualquier activo de información. Para el caso de los Contratistas y Terceros deben reportar los incidentes al Supervisor del contrato.

10. Todos los Empleados de Planta, Contratistas y Terceros deben aplicar la metodología de gestión de riesgos institucional, para identificar y tratar los riesgos de seguridad y privacidad de la información que puedan afectar a los activos de información a su cargo.

11. Todas las modificaciones o actualizaciones de los activos de información tecnológicos deben cumplir con el *Procedimiento de Gestión de Cambios*.

12. Todos los Empleados de Planta, Contratistas o Terceros de la Agencia Nacional Digital deben aplicar los controles de seguridad de la Información establecidos para tratar los riesgos que afectan la seguridad y privacidad de la información.

13. Todos los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital están obligados a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está sometida la Entidad para la protección de la información a su cargo.

14. Se consideran usos inapropiados sobre los activos de información, los siguientes:

    a. Incumplimiento de las políticas de seguridad y privacidad de la información y datos personales.
    b. Mal uso o abuso de los activos de información que se encuentran bajo su custodia o propiedad.
    c. Modificación de la información sin previa autorización.
    d. Divulgación no autorizada de información.
    e. Impedir el acceso a la información sin una justificación valida.
    f. Modificación o eliminación de los controles de seguridad.
    g. Cualquier acción sobre la información que sea considerada como ilegal o no autorizada por las leyes, regulaciones, normas o procedimientos a los que está sometida la Agencia Nacional Digital.
    h. Utilizar los activos de información de la Agencia Nacional Digital para fines personales o diferentes a los requeridos para el cumplimiento y desarrollo de las actividades o funciones laborales.

8.1.4. Devolución de Activos

Los Empleados de Planta, Contratistas y Terceros cuando se termine o cambie las condiciones de su contrato o acuerdo deben devolver los activos de información a su cargo conforme al *procedimiento de devolución de activos de información*, necesidades y requerimientos de la Agencia.

8.2. Clasificación de la Información

En la Agencia Nacional Digital debe establecer el nivel de protección de la información conforme a su importancia, requisitos legales, administrativos y operacionales de la misma, de acuerdo con la clasificación establecida.

8.2.1. Etiquetado de la Información

Todos los Empleados de Planta, Contratistas y Terceros cuando sea el caso, deben mantener organizado el archivo de gestión y digital, siguiendo los lineamientos establecidos por el proceso de Gestión

Documental, Seguridad y Privacidad de la Información, de acuerdo con la clasificación de la información establecida.

La plataforma tecnológica dispuesta para almacenar y conservar la información debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

Se debe definir el etiquetado de la información, de acuerdo con el esquema de clasificación definido por la Agencia Nacional Digital.

El etiquetado de información debe incluir la información física, electrónica y digital.

Las etiquetas de la información se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

8.2.2. Manejo de Activos de Información

La Agencia Nacional Digital debe realizar buen uso y manejo de la información y los datos personales que son procesados, almacenamos y transportados, teniendo en cuenta la clasificación de la información establecida.

Se debe restringir el acceso a la información de acuerdo con el nivel de clasificación que sea etiquetado.

Cada Proceso debe mantener un registro de la autorización de acceso a los activos de información.

El Proceso de Gestión de Tecnologías de la Información es responsable velar por el cumplimiento de la integridad, disponibilidad y confidencialidad de las copias de respaldo de información y datos personales, de acuerdo con los procedimientos y plan de copias de respaldo de información establecidos.

8.3. Manejo y Gestión de Medios Removibles

En la Agencia Nacional Digital se debe controlar la divulgación, modificación, retiro y destrucción no autorizada de la información almacenada en los medios de acuerdo con el *procedimiento de manejo de medios*.

Los medios removibles (USB, Discos Externos, cámaras fotográficas, cámaras de video, celulares, entre otros), que hacen parte de la operación de la Agencia deben ser controlados y gestionados de acuerdo con la clasificación de la información establecida.

La información de los medios de almacenamiento que ya no sea requerida para la operación de la Agencia Nacional Digital, debe ser eliminada de manera segura de acuerdo *procedimiento de eliminación segura de medios*.

Todo medio de almacenamiento previamente autorizado para su retiro de las instalaciones debe ser registrado en la recepción de las instalaciones y debe contar con la aprobación del supervisor, jefe inmediato o quien haga sus veces y contar con el aval de la Subdirección Administrativa y Financiera.

Los medios de almacenamiento deben tener un propietario asignado sobre este activo, y es su responsabilidad protegerlos y guardarlos con medidas de seguridad apropiadas en lugares seguros.

La información de la Agencia Nacional Digital contenida en los medios de almacenamiento debe estar cifrada, controlando el acceso de personal no autorizado.

Los propietarios de los medios de almacenamiento institucional deben informar previamente a la Subdirección Administrativa y Financiera el deterioro de los mismos o los riesgos que representa la información contenida en ellos, quien a su vez debe reportar al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales para que analicen el deterioro del activo y se generen las recomendaciones necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información.

En el caso que los Propietarios de los medios de almacenamiento de información institucional que requieran realizar copias de respaldo y/o bases de datos personales deben ser previamente autorizados por el Oficial de Seguridad de la Información y el Oficial de Privacidad de los Datos Personales, y realizadas de acuerdo con el *procedimiento de copias de seguridad de la información*.

Los medios de almacenamiento temporal (USB, DVD/CD, Discos Externos), deben utilizarse como copias de información sin dejar este medio como repositorio permanente de la misma.

El uso de medios de almacenamiento de la información debe ser restringido solo para personal autorizado. En cumplimiento con lo anterior, se bloqueará el acceso de puertos de medios de almacenamiento de acuerdo con las políticas establecidas y solo será habilitado a personal autorizado.

Cada Propietario de medios de almacenamiento removible es responsable de la transferencia de información que se hace en los mismos.

8.3.1. Disposición de los Medios

En la Agencia Nacional Digital se debe controlar la disposición de los medios de almacenamiento de forma segura cuando ya no sean requeridos para las operaciones o se encuentren en un estado de obsolescencia tecnológica.

Es responsabilidad de la Subdirección Administrativa y Financiera la custodia segura de los medios cuando son requeridos para su almacenamiento o conservación de los mismos por motivos de retiro, obsolescencia o cambio.

Los medios de almacenamiento que se encuentren en disposición de la Agencia Nacional Digital deben registrarse con el fin de mantener una trazabilidad sobre los mismos.

Todas las adquisiciones de hardware y software tecnológico se deben realizar previa autorización del Proceso de Gestión de Tecnologías de la Información.

8.3.2. Transferencia de Medios

En la Agencia Nacional Digital se debe asegurar la información que se transporta a través de los medios físicos protegiéndolos personal no autorizado frente la posible alteración del medio y de los datos.

Para el transporte de dispositivos o medios de almacenamiento fuera de las instalaciones debe realizarse con medidas adecuadas de seguridad, entre las que se establecen las siguientes:

- Contar con un contrato o acuerdo con una empresa de mensajería que disponga y provea los mecanismos de seguridad requeridos por la Agencia Nacional Digital para el transporte de medios.
- Definir los lineamiento y controles de seguridad que se deben cumplir para el transporte, procesamiento y almacenamiento de la información y los datos personales.
- Contar con un contrato o acuerdo con una empresa de almacenamiento de medios y copias de respaldo de información.
- Firmar los acuerdos de confidencialidad o transferencia de medios, con el fin de velar por el cumplimiento de las políticas de seguridad y privacidad de la información.

9. CONTROL DE ACCESO

9.1. Requisitos del Negocio para el Control de Acceso

La Agencia Nacional Digital debe limitar el acceso a la información, los sistemas de información e instalaciones de procesamiento para los Empleados de Planta, Contratistas y Terceros autorizados, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información y los datos personales. Así mismo, establece que la información debe estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso. En cumplimiento de lo anterior, establece la siguiente política conforme a los requisitos del negocio:

9.1.1. Política de Control de Acceso

La Agencia Nacional Digital ha establecido lineamientos de control de acceso con el fin de proteger la información de su uso por parte del personal no autorizado de acuerdo con los requisitos y necesidades organizacionales:

1. El Proceso de Gestión de Tecnologías de la Información, el de Gestión de Talento Humano, Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales, deben elaborar y hacer mantenimiento a la matriz de roles y permisos de acceso a los activos de información.

2. El Proceso de Gestión de Tecnologías de la Información debe proveer el acceso lógico y físico de acuerdo con las autorizaciones otorgadas por el responsable del activo y por medio de *Procedimiento de Seguridad física y del entorno*.

3. La Agencia Nacional Digital define el *Procedimiento de Gestión de Accesos* para todos los accesos que se requieran de red, correo, servicios, bases de datos, sistemas de información, aplicaciones y a cualquier servicio que disponga la Agencia.

4. Los privilegios de acceso, concedidos a los Empleados de Planta, Contratistas y Terceros a sistemas de procesamiento de información, aplicaciones, servicios de almacenamiento de información en Internet y tecnológicos, deben ser aprobados por la Subdirección o Líder de cada Proceso delegado.

5. Los privilegios deben limitarse al mínimo de permisos para cumplir con sus responsabilidades según lo determine su rol. Este acceso debe contemplar el tipo de permisos como son lectura, escritura, modificación, borrado o ejecución.

6. El Proceso de Gestión de Tecnologías de la Información valida los perfiles de usuarios limitando el acceso a la información de acuerdo con lo autorizado por los Líderes de Proceso sobre el control de la información de su área, teniendo en cuenta las tareas y la ejecución de las labores asignadas a cada usuario.

7. Todos los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital deben hacer buen uso de la conexión a las redes que le son autorizadas, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información y los datos personales.

8. Todo acceso físico o lógico, asignado a los Empleados de Planta, Contratistas y Terceros debe ser desactivado o modificado una vez se termina la autorización de uso sobre los mismos y tan pronto finalice el empleo, contrato o acuerdo por medio del *Procedimiento de Gestión de Accesos.*

9. Todos los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital deben contar con un identificador único (ID del usuario, Cuenta de usuario) para su uso personal, el cual es intransferible.

10. Los Líderes de Procesos con el apoyo de Seguridad de la Información y Tecnologías de la Información deben realizar las revisiones de los derechos de acceso otorgados, con el fin de asegurar la confidencialidad de la información.

11. Se deben establecer procedimientos para garantizar que se active los logs de auditoría de los sistemas, plataforma tecnológica, bases de datos y aplicaciones, con el fin de contar con la trazabilidad y registros ante cualquier incidente de seguridad de la información y para monitoreo de las acciones que se realizan con los usuarios.

12. Los Empleados de Planta, contratitas y Terceros deben abstenerse de instalar y utilizar herramientas o software que traten de evadir los controles de seguridad de los recursos tecnológicos y servicios de red de la Agencia Nacional Digital.

13. Los usuarios y claves de acceso son personales e intransferibles y no deben ser compartidos, en caso de que por fuerza mayor lo deban hacer, se debe dejar documentado y una vez se encuentre en la red de la Agencia debe realizar el cambio.

14. Los Empleados de Planta, Contratistas y Terceros deben establecer una contraseña segura, teniendo en cuenta la sección de Gestión de Contraseñas, con el fin de garantizar la seguridad de la información.

15. Se prohíbe la creación o habilitación de sesiones simultáneas de acceso para un mismo usuario.

16. Se debe disponer de un sistema central de monitoreo y control de logs de auditoria, donde se registren todos los eventos y acciones que realiza un usuario o el sistema, con el fin de identificar y alertar posibles amenazas de accesos y cambios no autorizados.

9.1.2. Acceso a Redes y a Servicios en Red

Se deben definir los roles y perfiles de acceso a la red y parametrizarlo en las herramientas que corresponda con el fin de contar con el control de los accesos que se otorgan.

No se debe realizar ninguna actividad de tipo remoto sin la debida autorización del proceso de Tecnologías de la Información.

Solo se debe permitir el acceso a las redes y servicios de la Agencia Nacional Digital al personal autorizado conforme a sus funciones y responsabilidades.

La conexión remota a la red de área local de la Agencia debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por el Grupo de Tecnologías de la Información, que cuenta con la auditoría habilitada, para realizar monitoreo, registro y trazabilidad de las actividades que se realizan.

Proteger las redes contra accesos no autorizados implementando mecanismos de control de acceso lógico y físico, monitoreo y generación de alertas.

Para el caso de la infraestructura contratada con Terceros (infraestructura nube pública, infraestructura nube privada), la Agencia Nacional Digital debe hacer cumplir los requisitos de control de acceso por medio de las cláusulas contractuales, acuerdos de confidencialidad y acuerdos de niveles de servicio.

La autenticación de usuarios remotos debe ser aprobada por el jefe inmediato, supervisor o quien haga sus veces del usuario solicitante y bajo una solicitud con su respectivo formato debidamente diligenciado.

Las redes inalámbricas de la Agencia Nacional Digital deben contar con métodos de autenticación robustos, y cifrado de la información para prevenir incidentes de seguridad.
Las redes inalámbricas de invitados deben estar separada de los Empleados de Planta y Contratistas.

9.2. Gestión de Acceso de Usuarios

La Agencia Nacional Digital debe asegurar el control de acceso de usuarios autorizados a la información, sistemas y servicios, restringiendo el acceso de personal no autorizado a través de mecanismos de sistemas de autenticación. Para redes externas, se deben definir mecanismos de control de acceso por medio de VPNs, Webservice, canales https, segmentación de redes o el que sea requerido de acuerdo con las necesidades del servicio. Así mismo, dicho acceso debe ser autorizado por el Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y del Proceso de Gestión de Tecnologías de la Información.

En los sistemas de información, aplicaciones, redes o cualquier servicio no se deben utilizar usuarios genéricos para su acceso.

Se debe establecer el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden realizar cambio de sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben tener una complejidad así:

- Contener Mayúsculas y minúsculas
- Números
- por lo menos un carácter especial
- Una longitud mayor a 9 caracteres
- Solicitar cambio cada 30 días
- No reutilizar las ultimas 6 contraseñas
- No debe tener caracteres consecutivos
- Time out debe ser de mínimo 3 minutos
- La contraseña debe almacenarse cifrada utilizando algoritmos de cifrado seguro

El usuario debe tener una complejidad así:

- Mínimo 7 dígitos
- Debe ser personalizado

Todas las claves de acceso que vienen predeterminadas por el fabricante se deben cambiar una vez se haya instalado y configurado el software o hardware (por ejemplo, apliance, impresoras, routers, switch, herramientas de seguridad, etc.).

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten.

Reportar a Seguridad de la Información sobre cualquier incidente o sospecha de que otra persona esté haciendo uso de su contraseña y usuario asignado.

Las contraseñas de acceso a los servidores y de administración a los Sistemas de Información, aplicaciones y herramientas tecnológicas y de seguridad deben ser cambiadas mínimo cada cuatro (4) meses.

Todo equipo de cómputo que requiera acceso a la red interna de la Agencia Nacional Digital debe tener como mínimo las siguientes medidas de seguridad: solución de antimalware instalada y actualizada, parches de seguridad al día y mecanismos de autenticación habilitado para el ingreso a la red.

9.2.1. Registro, Cancelación o revocación del Registro de Usuarios

Toda solicitud y/o cancelación de acceso de usuarios a la información, sistemas y servicios deben ser registrados a través del *formato de gestión de accesos*.

Las solicitudes de usuarios para acceso a la información, sistemas y servicios deben ser analizadas, evaluadas y asignadas por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales de acuerdo con las matrices de acceso definidas para los activos de información, roles y perfiles.

El encargado de los controles de acceso de los sistemas de información debe inactivarlos inmediatamente se le notifique la novedad por parte de la Subdirección Administrativa y Financiera en el cual se indica el retiro, cambio de rol o función del Empleado de Planta, Contratista o Tercero; o cualquier novedad que ponga en riesgo los activos de información.

Se debe enviar cada mes por parte del proceso de Gestión de Talento Humano a Seguridad de la Información las novedades administrativas (retiros, traslados, ingresos, incapacidades, vacaciones, etc.), con el fin de realizar la cancelación definitiva o temporal de los accesos.

Todo suministro o revocación de los derechos de acceso debe ser realizado con la autorización previa de la respectiva Subdirección, quien debe informar las causas o novedades sobre dicha solicitud.

La Agencia Nacional Digital se debe asegurar que se retiren los derechos de acceso de Empleados de Planta, Contratistas y Terceros que se hayan retirado, terminado sus contratos o por cambios realizados en los mismos.

9.2.2. Gestión de Derechos de Acceso Privilegiado

Para otorgar el acceso a usuarios privilegiados, se debe solicitar dando cumplimiento al procedimiento de Gestión de Accesos y diligenciar el formato de control de acceso.

Se debe restringir y controlar la asignación, uso y revocación de los derechos de acceso privilegiado al personal autorizado.

Se debe contar con mínimo doble factor de autenticación para fortalecer la seguridad de la información para los usuarios con altos privilegios.

9.2.3. Gestión de la Información Secreta para la Autenticación de Usuarios

Toda asignación de información de autenticación secreta (usuarios y contraseñas), se debe realizar a través de medios seguros de comunicación.

La información de accesos privilegiados debe entregarse y mantenerse almacenada con medios de cifrado, de acuerdo con la política de cifrado de la información.

Una vez sea entregado usuario y contraseña a los Empleados de Planta, Contratistas o Terceros, estos son responsables de mantener las condiciones de seguridad adecuadas.

La información secreta de autenticación es de uso personal e intransferible, por tal motivo, es responsabilidad de los Empleados de Planta, Contratistas y Terceros no compartirla y dar uso adecuado.

Se deben cambiar de inmediato las contraseñas genéricas dadas a los usuarios para su primer ingreso a los sistemas o recursos de información.

9.2.4. Revisión de los Derechos de Acceso de Usuarios

Los Propietarios de los activos de información deben revisar los derechos de accesos de los usuarios mínimos una vez al mes.

La revisión se debe realizar con el apoyo de los reportes o informes emitidos por los Sistema de Información o en su defecto por revisiones manuales que verifique el Propietario del Activo o encargado/delegado.

Es responsabilidad del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con sus equipos de trabajo revisar periódicamente mínimo una vez cada 6 meses o por demanda cuando se requiera validar los accesos establecidos en los activos de información frente a los derechos autorizados.

9.3. Responsabilidades de los Usuarios

Todos los Empleados de Planta, Contratistas o Terceros son responsables del manejo y protección de la información de autenticación.

Todos los Empleados de Planta, Contratistas y Terceros son responsables de guardar la confidencialidad de su información de registro en los sistemas de información.

Se debe evitar registrar la información de usuarios y contraseñas en papel o cualquier medio que pueda poner en riesgo la confidencial de acceso a los sistemas de información de la Agencia Nacional Digital.

Se debe cambiar la información de autenticación, en especial las contraseñas cuando se considere que hay un riesgo que compromete la misma.

Se deben definir contraseñas fuertes, de calidad, sencillas de recordar y difíciles de adivinar.

Las contraseñas deben cambiarse periódicamente en los tiempos establecidos por los sistemas automáticos o cuando sea requerido previendo cualquier riesgo sobre la información secreta.

Las contraseñas deben ser cambiadas en su primer ingreso a cualquier sistema de información.

No se debe usar la misma contraseña para el ingreso a varios sistemas de información. Ni usar las contraseñas de uso personal para uso institucional.

No se deben reutilizar las contraseñas para el acceso a los sistemas de información.

9.4. Restricciones de Acceso a la Información

El acceso a la información, sistemas y aplicaciones se debe restringir de acuerdo con las políticas de control de acceso y los requisitos propios de la aplicación. Para esto, se deben aplicar los siguientes requisitos:

- Las aplicaciones deben disponer de sistemas de autenticación que permitan el control de acceso a las mismas a través de usuario y contraseña que cuenten con la política de Gestión de Accesos a Usuarios.

- Se debe llevar el control de los accesos en los sistema y aplicaciones para los usuarios dependiendo su rol o función organizacional.

- Los permisos de acceso a la información deben restringirse en términos de lectura, escritura, actualización o modificación y borrado o eliminación, de acuerdo con los perfiles de usuario autorizados para dicha labor.

- Los sistemas y aplicaciones deben estar controladas frente al acceso de otras aplicaciones conforme a los requerimientos acordados.

- Se debe limitar en los sistemas y aplicaciones la información de salida, el cual sea la requerida por los procesos establecidos y para el personal autorizado.

- Se deben aislar los sistemas, aplicaciones y sistemas críticos con la aplicación de controles de acceso físico o lógico.

9.5. Control de Ingreso Seguro

El acceso a la información, sistemas y a las aplicaciones de la Agencia Nacional Digital se debe realizar a través de un *procedimiento de ingreso seguro*, incorporando sistemas de autenticación con usuario y contraseña, tokens, autenticación de doble factor, sistemas biométricos o cualquier mecanismo necesario requerido para un determinado caso.

Los sistemas de autenticación a los sistemas de información y aplicaciones deben ser analizados, evaluados y autorizados por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.

Los sistemas de autenticación deben mantener un registro o logs de auditoría que permita una trazabilidad de los ingresos y acciones realizadas.

Los sistemas de autenticación deben controlar el número de intentos fallidos que debe ser de 3.

Los sistemas de autenticación no deben emitir mensajes de ayuda que pongan en riesgo el acceso no autorizado a los sistemas de información.

Los sistemas de autenticación deben controlar los tiempos de conexión determinados de acuerdo con los riesgos al que se exponen la información.

Los sistemas de autenticación deben controlar las sesiones múltiples, restringiéndolas a un uso individual de las mismas.

Lineamientos Control de Ingreso Seguro en los Sistemas y Aplicaciones

En la Agencia Nacional Digital se establecen los siguientes lineamientos para el ingreso seguro a los sistemas y aplicaciones:

- No se deben visualizar los identificadores de ingreso al sistema o aplicación (usuario y contraseña.
- Se debe evitar emitir mensajes de advertencia.
- Se deben emitir mensajes de ayuda durante el proceso de ingreso siempre y cuando no se ponga en riesgo el ingreso no autorizado. Dichos mensajes deben ser evaluados y aprobados por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales como parte de los requisitos de seguridad y privacidad sobre el sistema o aplicación.
- Los sistemas o aplicaciones deben permitir solo el ingreso una vez se hayan completado los datos de entrada. En caso, que se identifiquen datos erróneos en el ingreso.
- No se debe emitir qué parte de los datos ingresados son los correctos o incorrectos por parte del usuario, ya que esto sería un indicador que pondría en riesgo el acceso no autorizado.
- Los sistemas o aplicaciones deben restrigir el acceso, bloqueando el ingreso a los tres (3) intentos fallidos, evitando los ataques de fuerza bruta.
- Los sistemas o aplicaciones deben llevar un registro a través de los logs de auditoría de los intentos exitosos y fallidos realizados por los usuarios.

9.6. Gestión de Contraseñas

La Agencia Nacional Digital debe establecer sistemas de gestión de contraseñas que permitan hacer cumplir y controlar el uso de las mismas en los sistemas de autenticación, asegurando su calidad y seguridad para un ingreso seguro.

Se debe contar con el registro centralizado de todos los accesos que se otorgan a los usuarios, el cual debe contener, fechas de inicio y fin de vigencia, datos del solicitante, tipo de acceso, tipo de usuario, permisos asignados, quien autoriza, entre otros.

El Proceso de Gestión de Tecnologías de la Información debe establecer e implementar controles que eviten múltiples intentos de autenticación fallida, como:

- Cambiar la contraseña por defecto en el primer ingreso
- Terminación de sesiones inactivas después de un período de inactividad de cinco minutos

9.7. Uso de Programas Utilitarios

En la Agencia Nacional Digital debe restringir y controlar el uso de programas utilitarios que pueden poner en riesgo la capacidad y operación de la información y los datos personales.

El Proceso de Gestión de Tecnologías de la Información y su equipo de trabajo son responsables de asegurar la configuración de los sistemas de información de la Agencia Nacional Digital, en el cual se realice la restricción y control de los programas utilitarios.

9.8. Control de Acceso a Códigos Fuente del Software

Los códigos fuente de todo el software desarrollado o adquirido a Terceros y que son de propiedad o uso de la Agencia Nacional Digital deben ser restringidos solo a personal autorizado.

Cualquier requerimiento de acceso a los códigos fuente debe ser previamente evaluado y autorizado por el Comité de Seguridad de la Información.

Los códigos fuente deben almacenarse en un repositorio, al cual sólo puede ingresar el personal autorizado.

10. CRIPTOGRAFÍA

10.1. Controles Criptográficos

La Agencia Nacional Digital debe asegurar el adecuado uso del cifrado de la información para preservar la confidencialidad e integridad de a información.

10.1.1 Uso de controles criptográficos

La Agencia Nacional Digital protege la confidencialidad, autenticidad e integridad de la información pública reservada o clasificada mediante controles criptográficos, de acuerdo con la normatividad y al *procedimiento de cifrado de la información*.
La Agencia Nacional Digital se deben utilizar controles criptográficos para para ofrecer servicios de seguridad:

- Servicios de autenticación.
- Servicios de confidencialidad.
- Servicios de integridad de los datos.

La Agencia Digital debe establecer cuales controles de cifrado debe aplicar la información y datos personales que son identificados como críticos después del análisis de riesgos.

10.1.2. Gestión de claves

La Agencia Nacional Digital establece las siguientes obligaciones para realizar la gestión y utilización segura de claves en los sistemas de información y plataformas de la Entidad:

Obligaciones:

1. Todos los Empleados de Planta de la Agencia Nacional Digital deben establecer una contraseña segura para el correo electrónico institucional y el acceso a las aplicaciones, servicios y plataformas o cualquier recurso general de información

2. Se debe cumplir con la política de Gestión de Accesos.

3. El usuario es responsable por la custodia de su contraseña, cada contraseña es de uso personal e intransferible. Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones por medio de la cuenta de otro usuario.

4. Todos los Empleados de planta o Terceros deben recibir junto con el nombre de usuario una clave para acceder a los recursos informáticos, la cual debe ser cambiada obligatoriamente en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma.

5. Está prohibido entregar la contraseña por el correo electrónico y/o mencionarla en una conversación ya que no son medios seguros. Si se sospecha que alguien ha obtenido acceso sin autorización a la cuenta se debe modificar la contraseña de forma inmediata.

6. Todos los Empleados de Planta o Terceros deben utilizar contraseñas diferentes en cada uno de los sistemas a los cuales tengan acceso.

7. Todos los Empleados de Planta o Terceros deben asignar la clave de acceso al equipo de cómputo asignado como lo determina el *Procedimiento Seguridad de equipos.*

8. El Proceso de Gestión de Tecnologías de la Información debe cambiar las claves de administrador de los diferentes sistemas con una periodicidad de 30 días.

9. El Proceso de Gestión de Tecnologías de la Información debe establecer controles para que después de tres intentos fallidos al digitar la clave del usuario, se bloquee de manera inmediata.

10. El Proceso de Gestión de Tecnologías de la Información debe establecer que el número de sesiones concurrentes de un mismo usuario sea limitado.

11. Todos los Empleados de Planta o terceros deben asegurarse de que las contraseñas no se encuentren de forma legible en cualquier medio impreso o dejarlos en un lugar visible donde personas no autorizadas puedan descubrirlas.

12. Las claves creadas por defecto por el fabricante del software o hardware deben ser cambiadas inmediatamente.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

La Agencia Nacional Digital controla el acceso a las áreas físicas y del entorno donde se desarrollan las operaciones, protegiendo sus activos de información.

11.1. Áreas Seguras

En la Agencia Nacional Digital se debe prevenir el acceso físico no autorizado, contra daño, interferencia de la información, a las instalaciones y áreas de procesamiento de información definiendo e implementando los controles necesarios en las áreas seguras, especialmente, en centros de cómputo, centros de gestión documental y áreas de procesamiento de información.

11.1.1. Perímetro de Seguridad Física

Se deben establecer las áreas de procesamiento con controles de seguridad que permitan la protección de los activos. De esta manera, se deben delimitar las áreas de procesamiento de la información de la Agencia Nacional Digital con la infraestructura necesaria para llevar a cabo las operaciones de una manera segura.

Todos los visitantes, sin excepción, deben portar la tarjeta de identificación de visitante o escarapela en un lugar visible mientras permanezcan en las instalaciones de la Agencia.

Es responsabilidad de todos Empleados de Planta, contratistas y terceros de la Agencia Nacional Digital borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

El horario autorizado para recibir visitantes en las instalaciones de la Agencia Nacional Digital es de 8:00 AM a 5:00 PM. En horarios diferentes se debe solicitar la autorización del Jefe de Oficina o responsable del Área que visita.

Los dispositivos removibles, así como toda información clasificada como Reservada, Reservada Clasificada, Confidencial, independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales los Empleados de Planta, contratistas y terceros no se encuentre en su sitio de trabajo.

Las instalaciones de la Agencia Nacional Digital deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de los Empleados de Planta, contratistas y terceros.

11.1.2. Controles de Acceso Físico

Se debe definir e implementar controles sobre las áreas de procesamiento de la información como centros de cableado, centro de datos, archivo, recepción y entrega de correspondencia de la Agencia Nacional Digital, mediante la implementación de mecanismos de control de acceso y uso de herramientas tecnológicas que permitan el control del acceso autorizado.

Para las áreas de procesamiento contratadas con un Tercero, la Agencia Nacional Digital debe exigir al proveedor los controles de acceso y de seguridad física necesarios que permitan protegerlas de acuerdo con las políticas establecidas.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un Empleado de panta o contratista del proceso.

El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

11.1.3. Seguridad de Oficinas, Recintos e Instalaciones

En la Agencia Nacional Digital se deben diseñar y aplicar los controles pertinentes para salvaguardar la seguridad física en sus oficinas e instalaciones de operación mediante la implementación de mecanismos y herramientas tecnológicas que restrinjan el acceso de personal no autorizado, por ejemplo, a través de sistemas biométricos, tarjetas de proximidad, sistemas de control de vigilancia, alarmas, sistemas de control de incendios, salidas de emergencia, entre otros, que sean requeridos.

Las áreas de procesamiento información (oficinas, centros de cómputo, áreas de archivo) de la Agencia Nacional Digital deben estar ubicadas estratégicamente, separadas y con controles de acceso físico que impidan el ingreso de personal no autorizado.

Las áreas críticas de procesamiento o almacenamiento de información como los centros de cómputo y áreas de archivo no deben tener señales que indiquen su ubicación o actividad que en estas se realizan. Así mismo, estas áreas deben tener controles físicos robustos con puertas seguras, sistemas de control de acceso (biométricos, tarjetas de proximidad, otros), y no ser visibles desde su exterior, evitando exponer la información y procesamiento de la misma a personal no autorizado.

Los números telefónicos o directorio de contactos de las áreas de procesamiento de información como los centros de cómputo y áreas de archivo solo deben ser proporcionados a personal autorizado.

11.1.4. Protección Contra Amenazas Externas y Ambientales

Para las instalaciones y áreas de operación de la Agencia Nacional Digital se deben diseñar e implementar controles de seguridad física adecuados que permitan proteger los activos de información contra amenazas externas y ambientales.

En la Agencia Nacional Digital se deben realizar capacitaciones y mantener asesorías con grupos especializados sobre temas de prevención y emergencia frente a posibles desastres causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles, entre otros que puedan afectar la Entidad.

11.1.5. Trabajo en Áreas Seguras

En la Agencia Nacional Digital se deben establecer controles de acceso físico y elementos idóneos que permitan un desarrollo normal y seguro de las operaciones. Para esto, se establecen los siguientes lineamientos:

Empleados de Planta, Contratistas y Terceros solo deben conocer las áreas, instalaciones o espacios necesarios para el ejercicio de sus funciones o realizar su trabajo.

Todo trabajo realizado por Empleados de Planta, Contratistas o Terceros autorizados, en las áreas críticas de procesamiento como Centros de Cómputo, Áreas de Archivo, entre otros que se definan en la Agencia, deben ser supervisados por su responsable de dicho espacio y a través de sistemas de monitoreo con cámaras de video.

No se permite, a no ser que sea autorizado, el ingreso de cámaras fotográficas, cámaras de video, dispositivos móviles, medios de almacenamiento (USB, Discos Externos, Memorias SD, etc), equipos de cómputo o cualquier elemento electrónico a las áreas críticas de procesamiento como Centros de Cómputo y Áreas de Archivo, entre otros que defina la Agencia.

11.1.6. Áreas de Despacho y Carga

En la Agencia Nacional Digital se debe establecer y realizar mantenimiento de las áreas de despacho y carga disponibles, restringidos de personal no autorizado y aislados de las áreas de procesamiento de información con la finalidad de recibir y realizar los envíos de encomiendas, paquetes o elementos de manera segura.

Las áreas de despacho y carga de la Agencia Nacional Digital deben disponer de controles de acceso restringiendo el ingreso de personal no autorizado. Complementario a lo anterior, se debe proveer de una identificación física a través de un carnet a los usuarios que pueden ingresar a dichas áreas.

En la Agencia Nacional Digital las áreas de despacho y carga deben estar separadas y aisladas del acceso a las áreas de procesamiento de la información de tal manera que se evite el acceso de personal no autorizado a las mismas.

Las áreas de despacho y carga deben disponer de puertas y seguridad para las mismas, de tal manera que se restrinja el acceso abierto de personal no autorizado. En caso de disponer de puertas internas en

las áreas de despacho y carga, estas deben permanecer cerradas cuando las externas se encuentren abiertas.

Todo material o elementos que lleguen al área de despacho y carga de la Agencia Nacional Digital se deben revisar e inspeccionar, con el fin de identificar posibles amenazas presentes en los mismos que puedan poner en riesgo los activos de información de la Entidad. Cualquier sospecha o alteración identificada se debe reportar de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información.*

Todo material o elementos que ingresan o se retiran del área de despacho y carga de la Agencia Nacional Digital deben llevarse en un registro de acuerdo con el *procedimiento de gestión de activos*.

Se deben separar el material o elementos que ingresan de los que salen en el área de despacho y carga.

11.2. Equipos

En la Agencia Nacional Digital se deben proteger los equipos contra pérdida, robo o cualquier afectación que pueda poner en riesgo la información o la continuidad de las operaciones.

11.2.1. Ubicación y Protección de los Equipos

Se deben establecer áreas y espacios adecuados para la ubicación y adecuación de los puestos de trabajo y equipos, protegidos del acceso no autorizado y de amenazas ambientales. Para esto se deben dotar de los elementos necesarios de protección para el uso seguro de los equipos como áreas cerradas y seguras, guayas para equipos móviles, entre otros elementos que se requieran para la operación.

Los equipos de la Agencia Nacional Digital deben ubicarse estratégicamente de tal manera que se mantenga el menor tráfico posible de personal sobre los mismos.

Las áreas de procesamiento de información sensible donde se encuentran los equipos críticos como servidores, o terminales que manejan bases de datos personales y de la Entidad, deben ser ubicadas estratégicamente, alejados de altos flujos de tránsito de personal y con controles de acceso el cual mitiguen al máximo el acercamiento de personal no autorizado.

Las áreas de almacenamiento de equipos en inventario, equipos de reutilización o que se encuentran para dar de baja deben disponer de controles de seguridad física, evitando el acceso de personal no autorizado.

Los equipos y medios de almacenamiento críticos (discos, cintas de copias de información, entre otros) deben estar identificados y resguardados en áreas seguras con los respectivos controles que eviten el contacto de personal no autorizado. Para esto se debe disponer de espacios protegidos como centros de cómputo.

Las áreas donde se encuentran los equipos deben contar con controles físicos, ambientales y de seguridad como: sistemas de control de incendios, controles de humedad, controles de temperatura, extintores, controles eléctricos, sistemas de monitoreo con video, salidas de emergencia, entre otras que se requieran para mantener un espacio adecuado para su funcionamiento en condiciones normales y seguras del entorno donde se encuentran.

En los puestos de trabajo o áreas de procesamiento de información de la Agencia Nacional Digital o las que la Entidad disponga se prohíbe el consumo de alimentos, bebidas, fumar o cualquier actividad que pueda poner en riesgos los activos de información.

Se deben monitorear los controles de ambientales (temperatura y humedad) donde se encuentran los equipos de la Agencia Nacional Digital, identificando cualquier alerta o novedad que pueda poner en riesgo los activos de información.

Se deben disponer de controles contra posibles descargas eléctricas sobre los equipos, implementando pararrayos en las instalaciones de la Agencia Nacional Digital y reguladores de energía en las redes eléctricas y de comunicaciones.

Se deben identificar e implementar los elementos de protección para los equipos de acuerdo con lo indicado por el fabricante y a las necesidades de la Agencia.

Los equipos y medios que procesan o almacenan información crítica o sensible deben ser protegidos contra amenazas electromagnéticas y fuga de información. Para esto, se deben implementar cifrado de datos y controles dados por los fabricantes.

11.2.2. Servicios de Suministro

Se deben disponer en la Agencia Nacional Digital de los servicios o elementos necesarios para el desarrollo normal de sus operaciones y la protección de los equipos contra fallas internas, falta de energía, fallas en las comunicaciones. En cumplimiento de lo anterior, se establecen los siguientes lineamientos:

Se deben mantener servicios de necesidad básica como: agua, energía, alcantarillado, gas (opcional). Y así mismo, servicios que permitan la operación de la Agencia como: telecomunicaciones (internet), aire acondicionado para áreas de procesamiento de información, entre otros, que requiera la Entidad para su operación.

Se deben mantener servicios de soporte y mantenimiento y elementos de contingencia como ups, plantas eléctricas alternas, operadores de internet alternos o con redundancia, entre otros.

Se deben cumplir los requisitos exigidos por los fabricantes de los equipos y legales vigentes sobre los mismos.

Se debe evaluar la capacidad de los servicios conforme a las necesidades actuales y proyectadas de la Agencia Nacional Digital.

Se deben hacer revisiones, mantenimientos y pruebas de los servicios conforme a lo emitido por el fabricante u operador prestador del mismo.

En lo posible se deben implementar sistemas de monitoreo sobre los servicios que permitan a la Agencia disponer de alarmas para detectar posibles fallas o deficiencia en los mismos. De manera especial, se requiere disponer de mecanismos de monitoreo sobre los servicios de energía y telecomunicaciones.

Para los servicios de energía y comunicaciones se debe disponer de redundancia en la prestación dichos servicios. Para el caso del servicio de agua en lo posible se debe disponer de una fuente de almacenamiento alterna que permita la provisión del mismo.

Se debe disponer de un sistema de iluminación y comunicaciones de emergencia independientes al principal.

Los interruptores de emergencia de los servicios en lo posible deben estar ubicados en las salidas de emergencia o en la salida de recintos, protegidos del personal no autorizado.

11.2.3. Seguridad en el Cableado

En la Agencia Nacional Digital se debe asegurar el cableado de todas las redes eléctricas y de comunicaciones conforme a las buenas prácticas establecidas en el mercado, con el fin de proteger el transporte de la información y continuidad de servicios tecnológicos de personal no autorizado. Para la seguridad en el cableado se establecen los siguientes lineamientos como mínimo:

Las redes de energía y de telecomunicaciones deben estar dentro de canaletas con consistencia fuerte de acuerdo con los requisitos exigidos por los fabricantes.

Las redes de energía deben estar separadas de las redes de telecomunicaciones con el fin de evitar interrupciones o fallas de operación normal de las mismas.

Los equipos o espacios críticos como centros de cómputo principal o alternos y cuartos de energía deben disponer de tuberías exigidas por el fabricante, cajas de interruptores con seguridad y blindaje electromagnético en caso de ser requerido.

Se deben realizar inspecciones técnicas de los dispositivos conectados en los sistemas de cableado.

Se debe restringir los paneles de control de los sistemas de cableado frente a posibles de acceso de personal no autorizado.

11.2.4. Mantenimiento de Equipos

En la Agencia Nacional Digital se debe realizar un mantenimiento y soporte a todos los equipos que hacen parte de sus operaciones conforme a las especificaciones de los fabricantes y buenas prácticas aplicadas.

Se debe planear los mantenimientos preventivos sobre los equipos de la Agencia y así mismo el registro de soportes realizados.

El mantenimiento y soporte de los equipos debe ser realizado por el personal autorizado, el cual debe disponer de las competencias técnicas para desarrollarlo.

Se deben registrar las fallas o sospechas identificadas sobre el mantenimiento preventivo y correctivo sobre los equipos.

Se deben definir controles de protección de la información, previo a mantenimientos de los equipos con el fin de protegerla del acceso de personal no autorizado.

Se deben realizar todos los mantenimientos de los equipos que exijan las garantías del fabricante o proveedor del mismo.

Se debe revisar y probar los equipos una vez termine su mantenimiento y validar su efectivo funcionamiento.

11.2.5. Retiro de Activos

Se debe llevar un control en el retiro de los activos de información con una autorización previa por parte del Propietario o responsable del mismo y la Subdirección Administrativa y Financiera. Para esto se establecen los siguientes lineamientos:

Se deben tener identificados todos los Empleados de Planta, Contratistas y Terceros que se encuentran autorizados para retirar equipos de la Agencia.

Se deben establecer los tiempos de retiro de los equipos para los Empleados de Planta, Contratistas y Terceros autorizados, y validar que se los mismos se cumplan.

Se debe registrar el retiro e ingreso de los equipos a las instalaciones de la Agencia Nacional Digital de documentando la identidad, rol y los activos asociados del usuario de acuerdo con el *procedimiento de control de acceso*.

La Subdirección Administrativa y Financiera con el apoyo del Oficial de Seguridad de la Información debe realizar revisiones periódicas sobre retiro de los activos.

En la Agencia Nacional Digital puede realizar revisiones a personal que ingrese o salga de sus instalaciones conforme a las disposiciones legales vigentes.

11.2.6. Seguridad de Equipos y Activos Fuera de las Instalaciones

El uso de equipos y activos de información fuera de las instalaciones de la Agencia Nacional Digital debe ser controlado conforme a las políticas de teletrabajo y dispositivos móviles; y a los riesgos asociados sobre el uso de estos como responsabilidad asumida por los usuarios autorizados.

Los equipos y medios de almacenamiento de información incluyen los computadores de escritorio, portátiles, tabletas, celulares, discos duros, USB, memorias SD, CD, DVD, y cualquier medio de almacenamiento propio de la Agencia o que opere en nombre de la misma.

El uso de los equipos o activos de información de propiedad de la Agencia Nacional Digital o los que obren en su nombre deben ser autorizados previamente por la Subdirección Administrativa y Financiera.

Los Empleados de Planta, Contratistas o Terceros autorizados para el uso de los equipos o activos de información fuera de las instalaciones deben cumplir los siguientes lineamientos:

- Los equipos y medios retirados son responsabilidad del Empleado de Planta, Contratista o Tercero autorizado y deben vigilarlos durante su uso en los diferentes sitios donde se encuentren.

- Es responsabilidad del Empleado de Planta, Contratista o Tercero autorizado debe proteger los equipos de amenazas informáticas, eléctricas y siguiendo los requisitos del fabricante.

- Es responsabilidad del Empleado de Planta, Contratista o Tercero identificar los riesgos e implementar los controles apropiados sobre el trabajo fuera de las instalaciones. Así mismo, acoger todas las recomendaciones de seguridad dadas por la Agencia Nacional Digital.

- Para el caso de transferencia de equipos entre Empleados de Planta, Contratistas o Terceros, el cual hayan sido previamente autorizados por la Subdirección Administrativa y Financiera, se debe llevar un registro como control de la transferencia y cadena de custodia de los mismos.

11.2.7. Disposición Segura o Reutilización de Equipos

En la Agencia Nacional Digital para la disposición o reutilización de equipos se deben verificar sus elementos de almacenamiento con el fin de identificar la información y prevenir cualquier acceso no autorizado a la misma. Para llevar a cabo este proceso, se deben realizar copias de seguridad y posteriormente el borrado de los datos de acuerdo con el *procedimiento de borrado seguro de la información*.

Para la disposición o reutilización de los equipos de establecen los siguientes lineamientos:

- Para la disposición o reutilización de los equipos se debe verificar que los mismos no contengan medios de almacenamiento. En tal caso, la información debe ser destruida de acuerdo con el *procedimiento de borrado seguro de la información*.

- La eliminación de los medios debe realizarse de acuerdo con el *procedimiento de eliminación segura de medios*, una vez se ha borrado de manera segura de información.
- Los equipos dañados que se requieran eliminar, previamente deben ser evaluados frente a los riesgos de pérdida de confidencialidad o fuga de información, y así definir los elementos a destruir en lugar de enviarlos a reparar o desechar.
- Se debe cifrar la información previamente al borrado de los medios con el fin de dar mayor seguridad en la eliminación de la información, minimizando aún más la probabilidad de recuperación de la misma por personal no autorizado.

11.2.8. Equipos de Usuario Desatendidos

El Proceso de Gestión de Tecnologías de la Información con su equipo de trabajo es responsable de configurar los sistemas de información con el fin de implementar controles sobre equipos desatendidos (siempre que los sistemas lo permitan), de tal manera que se inactiven las sesiones de los usuarios tan pronto identifiquen un periodo de inactividad de acuerdo con la criticidad del activo establecido.

Los usuarios de los equipos son responsables de asegurarse de cerrar sus sesiones cuando se alejen de sus equipos, abandonen su puesto de trabajo o por riesgos identificados de acceso a la información de personal no autorizado.

El Proceso de Tecnologías de la Información en las posibilidades que le brinden las aplicaciones, sistemas de información o servicios de red, debe configurarlas de tal manera que se cierren automáticamente una vez se identifique un periodo de tiempo de inactividad máximo de cinco (5) minutos, solicitando nuevamente las credenciales de autenticación.

11.2.9. Política de Escritorio Limpio y Pantalla Limpia

La Agencia Nacional Digital define esta política conforme a la clasificación de la información estableciendo las obligaciones necesarias para reducir riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o por fuera de las horas laborales a través de las siguientes obligaciones:

1. Los documentos físicos en papel o medios de almacenamiento electrónico (USB, CD, DVD, Discos Externos, entre otros), que contenga información confidencial, sensible o crítica se deben guardas de manera segura en las gavetas de escritorios o archivadores con llave, cuando ya no sea requerido, se

encuentre personal no autorizado, cuando se encuentre desocupada la oficina o cuando ya se aleja o se va de su puesto de trabajo.

2. Todos los equipos de la Agencia Nacional Digital deben ser bloqueados automáticamente después de cinco (5) minutos de inactividad o ser bloqueado por el usuario cuando no se encuentre en su puesto de trabajo y se exponga la información por presencia de personal no autorizado.

3. El uso de fotocopiadoras, impresoras, escáner, fax, o cualquier equipo de reproducción debe ser autorizado previamente por el Líder de Proceso, y establecer un control que permita llevar un registro sobre el uso de los mismos por parte de los usuarios.

4. Los documentos o medios que contienen información que sean generados por los usuarios a través de los medios de reproducción (fotocopiadoras, impresoras, escáner, fax, entre otros), deben ser retirados inmediatamente de los mismos para evitar divulgación no autorizada de la información.

5. Todos los Empleados de Planta o Terceros de la Agencia Nacional Digital son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma, de forma tal que solo se pueda desbloquear con la contraseña de usuario. Cuando finalice la jornada laboral, se deben cerrar todas las aplicaciones y dejar los equipos apagados o en hibernación.

6. Todos los Empleados de Planta o Terceros deben conservar su escritorio físico libre de información clasificada, que pueda ser tomada, copiada o utilizada por Terceros o personal sin autorización, cada vez que se vayan a retirar de sus puestos de trabajo.

7. Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave y/o utilizar una guaya de seguridad.

8. El Proceso de Gestión de Tecnologías de la Información debe aplicar controles de tiempo en las conexiones con los servidores de la Agencia Nacional Digital, solicitando nuevamente las credenciales de acceso después de un período de tiempo de inactividad del sistema.

9. Todos los Empleados de Planta o Terceros deben guardar en un lugar seguro cualquier documento y/o elementos de almacenamiento externos (CD, DVD, USB, Discos Externos, entre otros) conforme los niveles de clasificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

10. Los archivos que contengan información sensible o confidencial deben ser almacenados en rutas que impidan el fácil acceso por Terceros, evitando, guardarlos en el área de escritorio de la pantalla del computador.

11. El fondo del escritorio y protector de pantalla deben ser de uso institucional y no deben ser modificados sin autorización.

12. Todos los Empleados de Planta o Terceros que tenga dentro de sus responsabilidades la atención al público deben almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

12. SEGURIDAD DE LAS OPERACIONES

12.1. Procedimientos Operaciones y Responsabilidades

En la Agencia Nacional Digital se deben asegurar las operaciones de manera correcta y segura, a través de la definición de procedimientos sobre las operaciones.

12.1.1. Procedimientos de Operación Documentados

En la Agencia Nacional Digital se deben documentar, revisar y aprobar todos los documentos que hacen parte de sus operaciones de acuerdo con lo requerido en cada proceso y al sistema de gestión de calidad.

La Agencia Nacional Digital se deben disponer instrucciones sobre sus operaciones que incluyan lo siguiente:

- Instalación y configuración de las aplicaciones y sistemas de información.
- Manejo de información a nivel manual y electrónica a través de las herramientas tecnológicas implementadas.
- Copias de seguridad de la información.
- Requerimientos funcionales y requisitos de seguridad de la información para los desarrollos.
- Requisitos de programación relacionados con las actividades del proceso, interdependencia con otros sistemas y tiempos de finalización de la operación.
- Instrucciones de manejo de errores y restricciones de sobre las funcionalidades del sistema.
- Contactos de soporte y mantenimiento a nivel interno y externo.

- Instrucciones sobre el manejo de medios físicos y elementos de salida especiales (cheques, pólizas, entre otros).
- Instrucciones de reinicio y recuperación de sistemas en caso de fallas.
- Gestión de logs de auditoría a nivel de los sistemas de información y bases de datos.
- Instrucciones de seguimiento sobre las operaciones.

Todos los procedimientos de operación de la Agencia Nacional Digital deben ser documentados por los Líderes de Proceso, aprobados por la Dirección y publicados a los usuarios autorizados a través de los medios de comunicación establecidos.

Toda modificación o ajuste de los procedimientos de operación de la Agencia Nacional Digital debe ser realizado a través del *procedimiento de control de cambios*.

12.1.2. Gestión de Cambios

En la Agencia Nacional Digital se deben gestionar y controlar cualquier cambio en los activos de información que puedan afectar la seguridad y continuidad de las operaciones de acuerdo con el *procedimiento de gestión de cambios.*

Para la gestión de los cambios en los activos de información en la Agencia Nacional Digital se establecen los siguientes lineamientos:

- Todo cambio identificado y realizado deber ser registrado en el formato de control de cambios.
- Todos los cambios previos a ser realizados deben ser planificados, y una vez ejecutados deben ser probados en el ambiente de prueba establecidos por la Agencia.
- Todo cambio debe ser valorado frente a los riesgos e impactos potenciales que pueden causar a los activos en producción.
- Todo cambio debe tener una aprobación por parte de los responsables de los mismos de acuerdo con lo establecido en el *procedimiento de gestión de cambios*.
- Los cambios una vez realizados en los activos de información deben ser verificados frente al cumplimiento de los requisitos de seguridad de la información.
- Los cambios realizados deben ser comunicados a los responsables del mismo de acuerdo con el *procedimiento de gestión de cambios*.
- Se deben documentar controles de apoyo y responsabilidades sobre los mismos previendo casos no éxitos el cual se permita recuperarse frente a un evento adverso logrando volver a un estado estable del activo.

- Se debe definir controles de emergencia que permitan implementar de manera rápida y controlada cambios frente a incidentes que se puedan presentar.

Los cambios en los activos de información deben tener asignados responsables y funciones que permitan tener un control sobre los mismos.

Todo cambio debe ser registrado frente a su gestión desde su solicitud, apertura y cierre de acuerdo con el *procedimiento de gestión de cambios*.

Los cambios para ser aplicados en el ambiente de producción deben haber sido probados en el ambiente de pruebas.

Todo cambio que requiera pasarse al ambiente de producción debe haber cumplido con todas las actividades pertinentes de procedimiento de gestión de cambios y haber sido aprobado por los responsables del mismo.

12.1.3. Gestión de la Capacidad

La capacidad de los activos de información debe ser administrada por los Líderes de Proceso, asegurando la disponibilidad y el desempeño de las operaciones de la Agencia Nacional Digital.

Para la gestión de la capacidad se han establecido los siguientes lineamientos:

- Los requisitos de la capacidad deben definirse de acuerdo con la criticidad sobre los servicios prestados a nivel interno y externo por la Agencia.

- Se debe realizar monitoreo a los activos de información con el fin de identificar su desempeño y capacidad actual frente a operaciones futuras (próximas), el cual le permita a los Líderes de Proceso tomar decisiones anticipadas sobre la disponibilidad de la misma de acuerdo con las nuevas adquisiciones, tendencias de los sistemas y procesamiento de información de la Agencia.

- Los Líderes de Proceso deben determinar los tiempos de espera y costos para la adquisición de la capacidad planeada, de tal manera que le permita mantener la operación normal de los sistemas con los recursos vigentes durante un periodo prudencial frente al procesamiento de la información de la Agencia.

El Proceso de Gestión de Tecnologías de la Información debe administrar de manera adecuada los recursos tecnológicos para soportar o mejorar las operaciones. Para esto debe hacer un buen uso de los recursos tecnológicos aumentando la capacidad o disminuyendo la demanda, teniendo presente lo siguiente:

- Administrar los datos o información obsoletas para liberar espacio en disco.
- Cierres temporales o definitivos de los sistemas, bases de datos o ambientes de operación.
- Optimización de cronogramas.
- Procesamiento por lotes o agrupado.
- Optimización de consultas a bases de datos o aplicaciones.
- Restricción de anchos de banda de redes, dejando solo los servicios críticos en el uso de las mismas.

La gestión de la capacidad de los sistemas de información y redes de la Agencia Nacional Digital debe establecerse en el Plan de Tecnologías de la Información.

Cada Líder de Proceso debe incluir en su planeación la gestión de la capacidad a nivel de activos de información (Recurso Humano, Tecnología, Información, Infraestructura Física, Organizacionales), necesarios para el desarrollo de las operaciones propias de su proceso.

Los ambientes se deben poner a prueba y sus aplicaciones con el fin de validarlos previamente a ser utilizados.

12.1.4. Separación de los Ambientes de Desarrollo, Pruebas y Producción

En la Agencia Nacional Digital se deben mantener ambientes de desarrollo, pruebas y producción de manera separada con el fin de proteger la información que se maneja en la Agencia Nacional Digital. Para esto, se establecen los siguientes lineamientos:

Toda transferencia de software del ambiente de desarrollo al ambiente de pruebas; y de este al ambiente de producción debe haber cumplido todas las fases del *procedimiento de gestión de cambios*, especialmente, todas las aprobaciones pertinentes de dicho proceso.

El software de los ambientes de desarrollo, pruebas y producción deben funcionar en diferentes sistemas, procesadores, dominios y directorios.

Todo cambio previamente a ser puesto en el ambiente de producción debe ser validado en el ambiente de pruebas.

Los compiladores, editores y demás herramientas de desarrollo o utilidades de los sistemas deben restringirse para los sistemas que se encuentran en producción. En caso de ser requerido, debe haber autorización previa por parte del Oficial de Seguridad de la Información.

Los usuarios de los ambientes de desarrollo, pruebas y producción deben ser establecidos con diferentes perfiles de acceso para los mismos.

Cada ambiente debe disponer de controles de acceso pertinentes, con sistemas de autenticación con usuario y contraseña.

Los datos sensibles no deben utilizarse en los ambientes de desarrollo y pruebas. En caso de ser requerido, debe disponerse de la autorización del Oficial de Protección de Datos Personales y del Oficial de Seguridad de la Información.

12.2. Protección Contra Códigos Maliciosos

En la Agencia Nacional Digital se deben proteger los sistemas y aplicaciones contra códigos maliciosos que puedan poner en riesgo la seguridad y privacidad de la información, y la continuidad de las operaciones. Para esto, se deben implementar controles de prevención, detección y recuperación, toma de conciencia de los usuarios, controles de gestión de cambios y controles de acceso adecuados, considerando lo siguiente:

- Se prohíbe el uso de software no autorizado por la Agencia Nacional Digital.
- Se deben definir las listas blancas de aplicaciones, es decir, aquellas que son autorizadas para su uso.
- Se deben definir las listas negras con el fin de restringir el acceso a sitios web maliciosos.
- Se debe validar los riesgos de software realizando análisis o escaneos de archivos en ambientes de pruebas o redes externas al de producción.
- Se deben análisis de vulnerabilidades y escaneos con antivirus.
- Se deben revisar periódicamente el software instalado en los equipos. Dicha revisión debe mantener un registro donde se evidencia la actividad realizada y hallazgos encontrados.
- Se deben instalar antivirus a los equipos de la Agencia Nacional Digital.
- Se debe capacitar a los usuarios en el análisis de amenazas informáticas de sus equipos con el antivirus instalado en los mismos. Así mismo, sensibilizarlos sobre amenazas informáticas y la manera de prevenirlas con el fin de proteger la información de la Agencia.
- Los usuarios de los equipos deben escanear o analizar con el antivirus todo archivo que sea recibido por la red o medio de almacenamiento, con el fin de detectar software malicioso en los mismos. Y en caso de identificar un software malicioso no debe abrirse el archivo y notificar la novedad al Oficial

de Seguridad de la Información de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*.

- Los usuarios no deben abrir ningún archivo o enlace de internet sospechoso que identifiquen en sus correos electrónicos. Así mismo, dicha novedad debe ser reportada al Oficial de Seguridad de la Información de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información.*
- El Plan de Recuperación de Desastres debe incorporar instrucciones propias para enfrentar posibles ataques de amenazas informáticas, incluyendo copias de respaldo de software e información y dispositivos necesarios para la recuperación.
- Se debe investigar sobre las últimas amenazas informáticas o códigos maliciosos con entidades reconocidas como el COLCERT, la CVE entre otros, el cual le permitan a la Agencia mantenerse informada frente a las mismas.
- En caso de afectación de sistemas por causa de software malicioso se debe informar al Oficial de Seguridad de la Información y aislar su equipo de inmediato del ambiente de producción de acuerdo con las indicaciones dadas por el Proceso de Gestión de Tecnologías de la Información.

12.2.1 Controles Contra Códigos Maliciosos

En la Agencia Nacional Digital se deben implementar controles de detección, prevención y recuperación de códigos maliciosos. Así mismo, se debe sensibilizar a todos los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital sobre la prevención, protección y riesgos de los códigos maliciosos. Esta actividad es responsabilidad del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con sus equipos de trabajo deben analizar, evaluar y determinar las herramientas de seguridad y privacidad a aplicar en la Agencia Nacional Digital para proteger la información y datos personales contra códigos maliciosos.

El Proceso de Gestión de las Tecnologías de la Información es responsable de implementar y controlar las herramientas de seguridad aplicadas contra códigos maliciosos (antivirus, **antimalware**, entre otros).

12.3. Copias de Respaldo

En la Agencia Nacional Digital se debe proteger la información contra pérdida de la misma, asegurando su disponibilidad y la continuidad de las operaciones.

12.3.1. Respaldo de la Información

En la Agencia Nacional Digital se deben realizar copias de la información de trabajo, sobre el software, las configuraciones de los sistemas información y redes; y realizar las pruebas pertinentes de acuerdo con el *procedimiento de copias de seguridad de la información*.

Las copias de seguridad de la información y bases de datos personales deben almacenarse en activos diferentes a las cuales donde se realizó.

La Agencia Nacional Digital asegura que las copias de seguridad de la información y bases de datos personales sean creadas de acuerdo con los intervalos definidos y sean verificadas periódicamente, con el fin que la información este respaldada, protegida y disponible, dando cumplimiento a los siguientes lineamientos:

El Proceso de Gestión de Tecnologías de la Información es responsable de realizar las copias de seguridad y bases de datos personales, configuraciones y repositorios compartidos de todos los Empleados de Planta y Contratistas conforme al *procedimiento de copias de seguridad de la información*.

Cada Empleado de Planta es responsable de realizar las copias de seguridad de la información y bases de datos personales propia de su equipo o dispositivo. El Proceso de Gestión de Tecnologías de la Información para estos casos, sólo se hace responsable de backups realizados sobre los repositorios compartidos.

La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos de la Agencia Nacional Digital debe ser respaldada conforme a los lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como los niveles de clasificación de la información.

Los tiempos de preservación de las copias de seguridad deben ser definidos teniendo en cuenta los requerimientos de los procesos de la Agencia Nacional Digital, así como también la tecnología requerida para la restauración de la información contenida en las copias de seguridad. De esta manera, el Proceso de Gestión de Tecnologías de la Información debe revisar el estado de los medios de almacenamiento en las cuales se han realizado los backups de información, con el fin de mantener la disponibilidad de la información, realizando la respectiva migración de los datos cuando sea requerido a otro medio en caso de obsolescencia. Así mismo, los tiempos deben estar alineados con las tablas de retención documental.

Para la realización de copias de seguridad adicionales o nuevas a las estipuladas en el *procedimiento de copias de seguridad de la información*, el responsable de la información debe formular un requerimiento

al Proceso de Gestión de Tecnologías de la Información, determinando la necesidad de respaldo de información, el tipo de información a salvaguardar, frecuencia requerida para la toma de la copia de seguridad, niveles de clasificación de la información y el tiempo de retención de las copias. Dicha solicitud, debe ser evaluada por el Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y el Proceso de Gestión de Tecnologías de la Información.

Las copias de seguridad deben permitir que puedan restaurarse de forma completa y oportuna en caso de ser requerido. Para esto, el Proceso de Gestión de Tecnología de la Información debe hacer pruebas de restauración de los backups de manera periódica una vez cada trimestre. Para el caso de backups, realizados en la nube debe acordarse con el proveedor la prueba de restauración, y posteriormente realizar la validación por parte del supervisor del contrato.

El propietario del activo o custodio es el responsable de crear copias de seguridad de información bajo los lineamientos del *procedimiento de copias de seguridad* y las directrices dadas por el Proceso de Gestión de Tecnologías de la información.

Se deben registrar en un formato las actividades desarrolladas frente al tratamiento y manipulación de las copias de seguridad para asegurar la trazabilidad de mismas.

Las copias de seguridad de almacenamiento en medios físicos deben ser almacenadas en lugares con controles de seguridad física el cual dispongan de paredes robustas, control de acceso restringido de visitantes y personal no autorizado, sistemas de monitoreo y vigilancia por circuitos de televisión, sistemas de control de incendios y todas las medidas de emergencia y seguridad necesarias que permitan protegerlas.

Los Líderes de Proceso deben velar porque se realicen las copias de seguridad de la información y bases de datos personales de uso interno con la frecuencia que ha sido establecida en el *procedimiento de copias de seguridad de la información*.

Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de seguridad, estos medios deben ser eliminados o sometidos a disposición final de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas. Los procesos de eliminación o disposición final deben cumplir con la normatividad vigente en materia de dispositivos de residuos electrónicos. Para esto la Agencia Nacional Digital puede contratar servicios de empresas especializadas y certificadas en destrucción segura de la información.

El Proceso de Gestión de Tecnologías de la Información define las condiciones de transporte o transmisión y custodia de las copias de seguridad de la información y bases de datos personales que son almacenadas externamente.

Las copias de seguridad deben tener cifrado de la información con el fin de velar por la confidencialidad de la información.

Los Empleados de Planta o Terceros responsables de la infraestructura, sistemas de información y bases de datos requeridas para la operación de los procesos de la Agencia Nacional Digital, deben generar las respectivas copias de seguridad, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.

Se deben hacer una copia de seguridad del sistema antes de ejecutar cambios importantes en este.

Asegurar que los archivos no se estén utilizando durante el proceso de la copia de seguridad.

Los Empleados de Planta de la Agencia Nacional Digital deben almacenar la información requerida para sus procesos operativos, en la ubicación establecida por el Proceso de Gestión de Tecnologías de la Información, con el fin de garantizar la disponibilidad y copias de seguridad de cada uno de los procesos, así mismo, son responsables de depurar la información para la optimización de los recursos institucionales.

Las copias de seguridad y el proceso de restauración de estas deben ser probadas al menos una vez cada tres meses con la verificación de que todos los datos han sido recuperados satisfactoriamente.

12.4. Registro y Seguimiento

En la Agencia Nacional Digital se deben registrar los eventos sobre el procesamiento de la información con su respectiva evidencia.

12.4.1. Registro de Eventos

En la Agencia Nacional Digital se deben definir, conservar y revisar todos los eventos necesarios para llevar un control de la trazabilidad de los usuarios, fallas de seguridad en los sistemas y transacciones realizadas en las mismas.

Los registros de los eventos pueden incluir la siguiente información:

- Identificación de usuarios.
- Actividades del sistema.
- Fechas y horas en entradas y salidas al sistema, así como de operaciones realizadas.
- Identidad del dispositivo e identificador del sistema.
- Registros de intentos exitosos y fallidos al sistema.
- Cambios en la configuración del sistema.
- Uso de privilegios especiales.
- Uso de utilidades y funcionalidades del sistema.
- Información a la que se accedió.
- Direcciones y protocolos de red.
- Alarmas accionadas por el control de acceso.
- Activación y desactivación de los sistemas de protección como antivirus, IDS, IPS, entre otros.
- Registros de transacciones realizadas por los usuarios.

12.4.2. Protección de la Información de Registro

En la Agencia Nacional Digital se deben proteger todas las instalaciones de procesamiento y la información de registro contra las amenazas externas e informáticas conforme a las políticas de seguridad física y del entorno; y a las políticas de control de acceso.

Todo cambio en los registros debe ser autorizado por los responsables de acuerdo con el *procedimiento de gestión de cambios*.

Se debe realizar monitoreo sobre los registros de tal manera que se identifiquen los tipos de mensaje que se registran, la edición o eliminación de información; y sobre la capacidad de almacenamiento del medio del archivo que los contiene.

Los registros se almacenarán en repositorios seguros y se custodiarán por un tiempo definido en las tablas de retención documental.

Los registros que contengan información sensible deben ser cifrados con el fin de proteger su confidencialidad.

12.4.3. Registros de Administración y de la Operación

Los registros sobre la administración y operación de los sistemas se deben registrar y proteger del acceso no autorizado conforme a la clasificación y acceso a la información.

Los registros deben revisarse periódicamente mínimo cada tres (3) meses o cuando sea requerido, a través de muestras que permitan llevar un control sobre el uso especialmente de cuentas de acceso privilegiado.

12.4.4. Sincronización de Relojes

Todos los sistemas de información de la Agencia Nacional Digital deben estar sincronizados con la hora legal colombiana, asegurando el control adecuado del procesamiento frente a las operaciones de la Agencia Nacional Digital en términos de tiempo de ejecución. Esta hora debe ser establecida con la emitida por la Superintendencia de Industria de Comercio.

12.5. Control de Software Operacional

En la Agencia Nacional Digital se debe asegurar la integridad de la información y de los sistemas a través del control de las operaciones del software.

12.5.1. Instalación de Software en Sistemas Operativos

En la Agencia Nacional Digital se debe controlar la instalación del software en los sistemas operativos de los equipos.

El Proceso de Gestión de Tecnologías de la Información es el encargado realizar la instalación de software en los equipos de la Agencia Nacional Digital.

Toda instalación de software debe cumplir con la autorización previa de la Subdirección a la que pertenece la solicitud y del Oficial de Seguridad de la Información de acuerdo con el *inventario de software autorizado* en la Agencia Nacional Digital.

Los sistemas operativos solo deben contener códigos ejecutables del software y no código de desarrollo o compiladores.

Todo software previamente a la puesta en producción o de ser instalado en el mismo debe haber sido probado previamente por el Proceso de Gestión de Tecnologías de la Información.

El Proceso de Gestión de Tecnologías de la Información debe controlar el software implementado en los equipos y la documentación del mismo, mediante el uso de herramientas de control de software operacional.

El Proceso de Gestión de Tecnologías de la Información debe hacer pruebas de retroceso sobre el software a instalar de tal manera que pueda identificar maneras de corregir problemas sobre instalaciones fallidas o que impacten los sistemas.

El Proceso de Gestión de Tecnologías de la Información debe mantener un registro de auditoría de todas las actualizaciones del software.

El Proceso de Gestión de Tecnologías de la Información debe mantener todas las versiones del software adquiridas o desarrolladas por la Agencia, como medida de contingencia. Así mismo, deben ser conservados con los respectivos procedimientos, configuración y registro de soporte y mantenimientos realizados.

12.6. Gestión de vulnerabilidades

12.6.1. Gestión de las Vulnerabilidades Técnicas

La Agencia Nacional Digital establece la gestión de vulnerabilidades técnicas de manera oportuna con el fin de evaluar el grado de exposición y minimizar los riesgos asociados, cumpliendo con las siguientes obligaciones:

Obligaciones:

1. En la Agencia Nacional Digital se deben realizar pruebas de seguridad de la información a través de análisis de vulnerabilidades técnicas y pruebas de intrusión mínimo dos (2) veces al año sobre las plataformas y recursos tecnológicos actuales y nuevos de la Agencia Nacional Digital. Dichas pruebas pueden ser realizadas por el Oficial de Seguridad de la Información a manera de buena práctica y por medio de empresas especializadas contratadas por la Agencia Nacional Digital. Los resultados de las pruebas deben documentarse en la *Matriz de Vulnerabilidades Técnicas*.

2. El Oficial de Seguridad de la Información deben revisar los resultados e informes de las pruebas y definir el *plan de tratamiento de vulnerabilidades técnicas* con las acciones y responsables para su resolución de los hallazgos encontrados.

3. El Oficial de la Seguridad de la Información debe monitorear los planes de mitigación de las vulnerabilidades técnicas, validando con cada responsable el cumplimiento de las acciones

programadas y ejecutadas para la subsanación de las mismas, dando un cierre definitivo en el *plan de tratamiento de vulnerabilidades técnicas* cuando se encuentren a satisfacción.

4. Todos los Empleados de Planta de la Agencia Nacional Digital deben reportar oportunamente las vulnerabilidades que hayan sido detectadas al Proceso de Gestión de Tecnologías de la Información y al Oficial de Seguridad de la información a través del *formato de notificación y gestión de incidentes de seguridad y privacidad de la información*.

5. Todos los Empleados de Planta y Contratistas deben ejecutar mínimo semanalmente en sus equipos de cómputo y dispositivos móviles de la Agencia Nacional Digital o cuando sea requerido, los antivirus con el fin de analizar y detectar códigos maliciosos.

6. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben evaluar la relevancia y criticidad o nivel de urgencia de los parches para el entorno tecnológico, con el propósito de evitar fallas en la funcionalidad de los sistemas de información.

7. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben instalar los parches de seguridad críticos o ejecutar medidas de protección frente a vulnerabilidades que estén afectando a los sistemas que estén siendo vulnerados.

8. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben priorizar las vulnerabilidades críticas y de mayor impacto, mitigándolas lo más pronto posible.

9. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben hacer seguimiento de los parches de seguridad con las herramientas de gestión de vulnerabilidades y/o actualizaciones automáticas que provee la Agencia Nacional Digital.

10. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la Información, deben efectuar un análisis de riesgos previo para los cambios requeridos por vulnerabilidades críticas.

11. Antes de realizar cambios requeridos por vulnerabilidades críticas, el Proceso de Gestión de Tecnologías de la Información con el seguimiento del Oficial de Seguridad de la información, debe realizar las copias de seguridad de acuerdo con el *Procedimiento de Copias de Seguridad* para la disponibilidad de la información y ejecutar los cambios requeridos a través del *Procedimiento de Gestión de cambios*.

12. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben notificar previamente a las áreas involucradas sobre la implementación de un cambio que

pueda afectar las operaciones y a usuarios finales en pruebas de aceptación del nuevo estado por el cambio realizado.

13. El Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la información, deben definir e implementar las restricciones y controles de seguridad para uso e instalación de software a los usuarios en los equipos de cómputo y dispositivos móviles la Agencia Nacional Digital.

14. El Proceso de Gestión de Tecnologías de la Información es el responsable de realizar la instalación de software en los equipos de cómputo de la Agencia Nacional Digital, de acuerdo con el *Inventario de Software Autorizado* relacionado con su rol y funciones.

15. Quienes requieran la instalación de software adicional en equipos de cómputo específicos de la Agencia Nacional Digital deben realizar la solicitud inicialmente a su Jefe Inmediato, y este a su vez al Oficial de Seguridad de la Información con la debida justificación, quien a su vez debe evaluar y autorizar o no dicha solicitud de acuerdo con lo establecido en el *Procedimiento de Gestión de Cambios*. En caso de ser autorizada, el Oficial de Seguridad de la Información debe actualizar el Inventario de Software Autorizado con el Proceso de Gestión de Tecnologías de la Información el cual debe pasar a aprobación por parte del Comité de Seguridad de la Información. Posteriormente, el Proceso de Gestión de Tecnologías de la Información debe proceder a realizar dicha instalación.

16. El Proceso de Gestión de Tecnologías de la Información debe realizar y mantener un inventario actualizado del software autorizado para instalar en los equipos de cómputo de la Agencia Nacional Digital. Dicho inventario previamente debe ser autorizado por el Comité de Seguridad de la Información.

17. El Oficial de Seguridad de la información con cada Proceso, debe definir los niveles de accesos con privilegios especiales en el software y aplicaciones de la Agencia Nacional Digital.

12.6.2. Restricciones sobre la Instalación de Software

En la Agencia Nacional Digital se debe restringir la instalación del software en los equipos de la Agencia Nacional Digital, conforme al *Inventario de Software Autorizado*.

El Proceso de Gestión de Tecnologías de la Información con su equipo de trabajo son los encargados de instalar el software en los equipos de los usuarios de acuerdo con el *Inventario de Software Autorizado* para el Empleado de Planta, Contratista o Tercero conforme a sus funciones con la Agencia Nacional Digital.

La instalación de software debe ser autorizada previamente por el Oficial de Seguridad de la Información, quien a su vez es encargado de realizar revisiones periódicas mínimo cada tres (3) meses o cuando tomando muestras aleatorias de equipos de la Agencia Nacional Digital, a los cuales debe validar el software instalado en los mismos conforme al *Inventario de Software Autorizado*.

12.7. Consideraciones sobre Auditorías de Sistemas de Información

En la Agencia Nacional Digital deben realizar auditorías a los sistemas de información de manera precavida minimizando el impacto de las mismas en las operaciones.

12.7.1. Controles sobre Auditorías de Sistemas de Información

En la Agencia Nacional Digital Control Interno con el apoyo del Oficial de Seguridad de la Información deben definir y acordar los requisitos y actividades de las auditorías a los sistemas de información buscando minimizar los riesgos y el impacto en las operaciones. Para esto se establecen los siguientes lineamientos:

- Se debe acordar con la Subdirección o Líder de Proceso responsable del software los requisitos de auditoría para el acceso a los sistemas y datos almacenamos en los mismos.

- Se debe definir el alcance de pruebas técnicas de auditorías sobre los sistemas, asegurando la ejecución de las mismas de manera segura y evitando posibles impactos en los mismos.

- Las pruebas de auditoría sobre los sistemas se deben limitar solo al acceso y consulta de datos. En caso que se requieran permisos diferentes al de lectura, se debe disponer de autorización del responsable del sistema y de la información que almacena el mismo. Una vez terminadas las pruebas debe eliminarse el acceso proporcionado para la auditoría.

- El Auditor es responsable de cualquier evidencia recolectada en las pruebas de auditoría a los sistemas evaluados.

- En caso de auditorías a procesos críticos deben ser acordados previamente con propietario o responsable del mismo, con el fin de considerar elementos adicionales a tener presente para el desarrollo de las actividades pertinentes.

- Las pruebas de auditoría que puedan afectar la disponibilidad del servicio de los sistemas deben ser realizadas en horarios fuera de los laborales o en espacios que no afecten las operaciones de la Agencia.

- Las auditorías de los sistemas deben considerar el seguimiento de los accesos y registrarlos como referencia. Así mismo, los accesos de la auditoría como evidencia sobre este proceso realizado.

13. SEGURIDAD DE LAS COMUNICACIONES

13.1. Gestión de la Seguridad de las Redes

En la Agencia Nacional Digital se debe proteger la información que viaja a través de las redes de comunicación e instalaciones de procesamiento, a través de la implementación de los siguientes controles:

13.1.1. Controles de Redes

Se debe mantener un control y gestión sobre la información que transita en las redes de comunicación, sistemas y aplicaciones conforme a las políticas de control de acceso, políticas de cifrado y políticas a nivel de infraestructura de seguridad a través de herramientas tecnológicas como: firewalls, vpns, https, canales cifrados, entre otros que se consideren necesarios.

Los controles de seguridad en las redes a nivel tecnológico deben ser definidos por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales e implementados por el Proceso de Gestión de Tecnologías de la Información y su equipo de trabajo.

Las redes de comunicaciones de la Agencia Nacional Digital deben disponer de sistemas de autenticación segura a través del manejo de protocolos de seguridad y contraseñas fuertes de acuerdo con lo establecido en la *política de control de acceso* del presente documento.

Las redes de comunicaciones de la Agencia Nacional Digital deben disponer de registros o logs de auditoría que permitan tener una trazabilidad de las operaciones realizadas sobre las mismas.

Las redes de comunicaciones deben disponer de sistemas de monitoreo que permitan llevar una gestión sobre el comportamiento de las mismas.

Los sistemas de redes de comunicaciones se deben autenticar y restringir el acceso a usuarios no autorizados.

- **Roles y Responsabilidades de Control de las Redes**

Para el control de las redes se han establecido los siguientes roles y responsabilidades:

- **Proceso de Gestión de Tecnologías de la Información**

Es encargado de diseñar, implementar y monitorear las redes de comunicación que hacen parte de la Agencia Nacional Digital.

Gestionar y supervisar contratos de servicios de redes de comunicaciones establecidos con Terceros operadores.

Asegurar la correcta configuración de las redes de comunicaciones en términos de capacidad, disponibilidad y seguridad de las mismas.

Controlar los cambios requeridos sobre la infraestructura de las redes de comunicaciones de acuerdo con el *procedimiento de gestión de cambios*.

Identificar, reportar y gestionar riesgos e incidentes relacionados con las redes de comunicaciones, conforme al *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*.

Direccionar, gestionar y asegurar el mantenimiento preventivo de las redes de comunicaciones.

Realizar monitoreo a las redes de comunicaciones, de tal manera que pueda identificar su comportamiento y alertas de las mismas frente a su funcionamiento o riesgos de seguridad y privacidad sobre las mismas.

Direcciones y gestionar el soporte tecnológico sobre las redes de comunicaciones, con el fin de brindar a los usuarios la disponibilidad del servicio adecuado para el desarrollo de sus operaciones normales de su trabajo.

El Proceso de Gestión de Tecnologías de la Información debe proteger y mantener segura toda la información de configuración y autenticación de las redes de comunicaciones.

- **Profesionales de Tecnologías de la Información**

Apoyar actividades de monitoreo de las redes de comunicaciones.

Aplicar configuraciones de las redes de comunicaciones dirigidas y guiadas por el Proceso de Gestión de Tecnologías de la Información.

Atender requerimientos de soporte y mantenimiento de las redes de comunicaciones.

Reportar al Proceso de Gestión de Tecnologías de la Información los riesgos, incidentes o vulnerabilidades tecnológicas y de seguridad sobre las redes de comunicaciones.

El Profesional de Tecnologías de la Información debe proteger y mantener segura toda la información de configuración y autenticación de las redes de comunicaciones que se encuentre bajo su responsabilidad.

- **Oficial de Seguridad de la Información y Oficial de Protección de Datos Personales**

Definir estrategias de seguridad y privacidad de la información para la implementación en las redes de comunicaciones, el cual permitan asegurar la protección de la información y de los datos personales.

Realizar con el equipo de seguridad el monitoreo de incidentes de seguridad de la información y privacidad de los datos personales presentados en las redes de comunicaciones.

Realizar cuando sea requerido, revisiones a través de pruebas de seguridad y privacidad a la infraestructura de seguridad establecida en las redes de comunicaciones.

Definir y validar requisitos de seguridad y privacidad de la información en la contratación de servicios de redes de comunicaciones contraídos con Terceros.

Informar al Proceso de Gestión de Tecnologías de la Información los requisitos de seguridad y privacidad de la información necesarios para asegurar las redes de comunicaciones.

Direccionar, gestionar y supervisar pruebas de seguridad y privacidad de la información y los datos personales a través de análisis de vulnerabilidades y pruebas de intrusión sobre las redes de comunicaciones.

Realizar revisiones a los logs de auditoría emitidos por las redes de las comunicaciones en términos de seguridad y privacidad de la información sobre las mismas.

Realizar y hacer seguimiento a planes de mejoramiento sobre la mitigación de vulnerabilidades técnicas sobre las redes de comunicaciones, con el fin de fortalecer la seguridad y privacidad de la información.

Llevar a Comité de Seguridad de la Información y Privacidad de Datos Personales estrategias e incidentes de seguridad de la información y privacidad de datos personales en las redes que puedan poner en riesgo la misión, visión u operaciones de la Agencia Nacional Digital.

- **Profesional de Seguridad de la Información**

Apoyar la implementación de las estrategias de seguridad de la información definidas para las redes de comunicaciones.

Realizar monitoreo al cumplimiento de los requisitos de seguridad de la información aplicados en las redes de comunicaciones e informarlo de manera oportuna al Oficial de Seguridad de la Información.

Apoyar el seguimiento a los requisitos de seguridad de la información de los servicios de redes de comunicaciones adquiridos con Terceros.

Apoyar el desarrollo de pruebas de seguridad y análisis de vulnerabilidades sobre las redes de comunicaciones.

Apoyar el seguimiento de cumplimiento de aplicación de controles para la mitigación de vulnerabilidades sobre las redes de comunicaciones.

Realizar seguimiento a logs de auditoría sobre el comportamiento de los elementos de seguridad de la información que hacen parte la infraestructura tecnológica de las redes de comunicaciones.

- **Usuarios de las Redes de Comunicaciones**

Todos los Empleados de Planta y Contratistas autorizados para uso de las redes de comunicaciones de la Agencia Nacional Digital son responsables de dar buen uso a las mismas. Por tanto, deben utilizarlas para uso de su trabajo en cumplimiento de sus funciones y responsabilidades.

Todos los Empleados de Planta y Contratistas deben reportar de manera oportuna los incidentes, riesgos o vulnerabilidades detectadas en las redes de comunicaciones de la Agencia Nacional

Digital. Esto debe hacerse de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*.

Todos los Empleados de Planta y Contratistas no deben acceder a redes de la Agencia Nacional Digital sin la debida autorización dada por el Oficial de Seguridad de la Información de acuerdo con la *Matriz de Acceso a Activos de Información*. Así mismo, cualquier intrusión o vulneración de los permisos a las mismas sin la debida autorización, puede ser considerada como un incumplimiento a las políticas de seguridad y privacidad de la información, según sea el caso y debe ser tratado como un incidente de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*.

13.1.2. Seguridad de los Servicios de Red

En la Agencia Nacional Digital se debe disponer de mecanismos de seguridad y requisitos de gestión de los servicios de red, a través del establecimiento de acuerdos de nivel operativo o de nivel de servicio a nivel interno o externo cuando se contrate un Tercero. De esta manera, el Proceso de Gestión de Tecnologías de la Información debe velar porque los acuerdos se cumplan.

El Proceso de Gestión de Tecnologías de la Información debe gestionar la capacidad del proveedor de los servicios de redes de comunicaciones, haciéndole el debido seguimiento y monitoreo de las mismas.

El Proceso de Gestión de Tecnologías de la Información para la contratación de servicios de redes de comunicación debe incluir en sus contratos, acuerdos o convenios el derecho de realizar auditorías cuando se requiera al proveedor sobre el servicio contratado.

Las redes de comunicaciones de Agencia Nacional Digital deben disponer de elementos de seguridad que permitan blindar y proteger la información que transita por las mismas. Para esto, es necesario que se apliquen certificados de seguridad sobre los canales de comunicación, firewalls, IPS, IDS, y/o cualquier herramienta tecnológica que mantenga la seguridad de las mismas.

Las redes de comunicación de la Agencia Nacional Digital deben disponer de controles de seguridad sobre los servicios como autenticación, cifrado de la información y controles de conexión de red, el cual la restrinjan de personal no autorizado y la protejan de amenazas informáticas.

Las redes de comunicación de la Agencia Nacional Digital deben tener una autenticación segura a través de aplicación de reglas de control de conexión de acuerdo con la *política de control de acceso* de este documento.

En la Agencia Nacional Digital se deben restringir el acceso a las redes y servicios de red conforme a los roles y perfiles de usuario establecidos en la *Matriz de Control de Acceso a Activos de Información*.

13.1.3. Separación en las Redes

En la Agencia Nacional Digital se deben mantener separados los servicios de información, usuarios y sistemas de información en las redes. La separación de estos recursos en las redes es responsabilidad del Proceso de Gestión de Tecnologías de la Información.

El Oficial de Seguridad de la Información con su equipo de trabajo pueden realizar revisiones o monitoreo cuando se requiera sobre la separación de estos recursos en la red.

En la Agencia Nacional Digital se deben separar las redes por dominios de red, determinando por ejemplo: el dominio público, dominio privado, dominio en la nube, dominio de escritorio, dominio de servidor, o cualquiera según la necesidades de las operaciones. Cualquier implementación o cambio en estos dominios debe ser acordada y aprobado de acuerdo con el *procedimiento de gestión de cambios*.

En la Agencia Nacional Digital se pueden implementar redes de comunicaciones en ambientes físicos, virtuales o en la nube, propias o con Terceros, con los respectivos controles de seguridad dependiendo el contexto. De acuerdo con lo anterior se establece lo siguiente:

- Todas las redes de comunicaciones físicas que están soportadas en activos tecnológicos propios de la Agencia Nacional Digital o contratadas con Terceros deben cumplir con las *políticas de seguridad física* establecidas.
- Las redes de comunicaciones virtuales deben disponer de controles de seguridad de la información y privacidad de los datos personales como: controles de acceso con sistemas de autenticación fuerte, cifrado de canales y de datos, registros de logs de auditoría, sistemas de monitoreo, estar segmentadas de acuerdo con los servicios establecidos para la Agencia Nacional Digital.
- Las redes de comunicaciones que son contratadas con activos tecnológicos de Terceros deben ser controladas por el Proceso de Gestión de Tecnologías de la Información. Para esto, debe:

    - Establecer acuerdos de confidencialidad de la información.
    - Establecer acuerdos de tratamiento de datos personales.
    - Realizar monitoreo a las mismas.
    - Exigir los acuerdos de niveles de servicio establecidos con el proveedor, asegurando la disponibilidad del servicio a los usuarios.

- Configurar y administrar los parámetros de las redes de comunicaciones de acuerdo con las necesidades funcionales y de seguridad de la información y privacidad de los datos personales de las mismas.
- Mantener un contacto permanente con el proveedor en caso de requerir soporte y mantenimiento en las mismas.

- La separación de las redes de la Agencia Nacional Digital debe permitir establecer y permitir el control perimetral de las mismas. Dichos perímetros de las redes deben ser definidos por el Oficial de Seguridad de la Información e implementados por el Proceso de Gestión de Tecnologías de la Información.
- La separación o segmentación de las redes de comunicaciones deben ser analizadas y evaluadas conforme a la clasificación de la información, control de accesos, riesgos, criticidad de los servicios, impactos sobre el desempeño en las tecnologías de la información aplicadas.

Las redes de comunicaciones de la Agencia Nacional Digital deben estar segmentadas de tal manera que se aíslen los activos críticos, estableciendo zonas desmilitarizadas (DMZ). Esta actividad debe ser realizada por el Oficial de Seguridad de la Información con el Proceso de Gestión de Tecnologías de la Información.

13.2. Transferencia de Información

En la Agencia Nacional Digital se debe proteger la información y los datos personales que sean transferidos a nivel interno o externo, a nivel físico o lógico.

13.2.1. Políticas y Procedimientos de Transferencia de Información

La Agencia Nacional Digital debe proteger la información durante su intercambio a nivel interno entre los Empleados y a nivel externo con Contratistas y Terceros, preservando las características de disponibilidad, integridad y confidencialidad. Para ha esto ha definido los siguientes lineamientos:

La transferencia o intercambio de la información de la Agencia Nacional Digital se debe controlar de acuerdo con los niveles de clasificación de la información establecidos en el *procedimiento de clasificación y etiquetado de la información*.

Todos los Empleados de Planta o Terceros deben utilizar únicamente los mecanismos y herramientas autorizadas por el Oficial de Seguridad de la Información, el Oficial de Protección de Datos Personales y proporcionadas por el Proceso de Gestión de Tecnologías de la Información para el envío o recepción de

información de la Agencia Nacional Digital de acuerdo con el *Procedimiento Transferencia o intercambio de información*.

Los Empleados de Planta o Terceros no deben revelar o intercambiar información confidencial de la Agencia Nacional Digital por ningún medio, sin contar con la debida autorización del Jefe del Área, Supervisor y/o responsable del activo de información.

Los Supervisores de los contratos o convenios que requieran un intercambio de información con entidades externas deben realizarlo cumpliendo las Políticas de Seguridad y privacidad de la Información de la Agencia Nacional Digital, estableciendo acuerdos de intercambio de información con el Tercero y siguiendo el *Procedimiento Transferencia o intercambio de información*. Así mismo, cualquier intercambio de información debe ser evaluado y autorizado previamente por Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.

La transferencia o intercambio de información debe realizarse protegiendo la confidencialidad e integridad de los datos de acuerdo con la clasificación del activo y el tipo de información involucrada.

Antes de realizar la transferencia de cualquier tipo información, el Supervisor del contrato o encargados delegados deben realizar el análisis con el software antivirus y antimalware, para verificar que no esté comprometido con algún tipo de código malicioso.

En caso de que se requiera intercambiar información sensible (datos de la Agencia o de datos personales), previamente autorizada por el propietario o responsable de la información, se deben adoptar controles de cifrado de información de acuerdo con lo establecido en la *Política de Criptografía* para preservar la confidencialidad, integridad y disponibilidad de la información durante su transferencia.

Todos los Empleados de Planta o Contratistas deben abstenerse del envío de archivos que contengan extensiones ejecutables y otras que puedan ser utilizadas para envío de códigos maliciosos, por medio del correo electrónico de la Agencia Nacional Digital.

Para la transferencia de información el Supervisor del contrato o personal delegado con el apoyo Oficial de Seguridad de la Información debe tratar los riesgos relativos al uso de canales de comunicación de forma que se mantengan los niveles de seguridad aceptables para los responsables de los datos. En cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), se debe realizar a través de canales que preserven los niveles de confidencialidad e integridad de la información, conforme al nivel de calificación de la información trasmitida.

13.2.2. Acuerdos sobre Transferencia de Información

En la Agencia Nacional Digital los intercambios de información con otras entidades deben estar soportados por medio de contratos, convenios o acuerdos formalizados, determinando en ellos los medios, controles en el tratamiento de la información y contener cláusulas que coincidan con la evaluación de riesgos, como el método de identificación de la otra parte, autorizaciones para acceder a la información, estándares técnicos para la transferencia de datos, respuesta a incidentes, etiquetado y manejo de información sensible, y derechos de autor. Así mismo, se deben firmar acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas, incluyendo los compromisos adquiridos y las penalidades por el incumplimiento de dichos acuerdos.

Los acuerdos de transferencia de información deben incluir lo siguiente:

- Las responsabilidades de la Dirección de la Agencia para controlar y notificar la transferencia, envío y recibo de la misma.
- Procedimientos para asegurar trazabilidad y no repudio.
- Mecanismos de envío seguro para la transmisión, por ejemplo, con cifrado de la información.
- Certificados de títulos en garantía (cuando aplique).
- Estándares de identificación de la mensajería que se utilice para la transmisión.
- Responsabilidades frente incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.
- Lineamientos de registro y lectura de la información, software y medio para aplicar la transmisión.
- Cifrado de la información para datos sensibles personales y de la operación de la Agencia.
- Mantener una cadena de custodia para la información en tránsito.
- Establecer controles de acceso sobre la información en tránsito.

13.2.3. Acuerdos de Confidencialidad

En la Agencia Nacional Digital se deben identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad el cual manifiesten la protección de la información por parte de la Entidad conforme a los requisitos legales y contractuales.

Para los acuerdos de confidencialidad se tendrán presentes los siguientes lineamientos:

- Establecer una definición información confidencial (la que se va a proteger y compartir de manera segura).
- Tiempo del acuerdo de confidencialidad (temporal o permanente=.
- Acciones cuando termine el acuerdo o contrato.
- Responsabilidades de la Agencia y el Empleado de Planta, Contratista o Tercero.
- Derechos sobre la realización de auditorías.
- Notificación en casos de incidentes sobre la información.
- Plazos o tiempo de devolución de la información.
- Procedimientos de destrucción o eliminación segura de la información.
- Penalizaciones en caso de incumplimiento sobre el acuerdo.
- Se deben firmar actas de confidencialidad con los Empleados de Planta, Contratistas o Terceros que por diferentes razones requieran conocer o intercambiar información clasificada y reservada. En estos acuerdos deben especificarse las responsabilidades para el intercambio de la información para cada una de las partes y se deben firmar antes del acceso o uso de dicha información.
- El uso de la información transmitida o intercambiada se debe realizar conforme a las características del contrato, convenio o acuerdo suscrito con el Tercero y cumpliendo la normatividad vigente en materia de protección y tratamiento de datos.
- La transmisión de la información se debe realizar teniendo en cuenta la normatividad colombiana vigente, como la Ley de Habeas Data Ley 1266 de 2008 y sus decretos reglamentarios, la Ley de Protección y tratamiento de Datos Personales Ley 1581 de 2012 y decretos reglamentarios.

13.2.4. Mensajería Electrónica

Los Empleados de Planta, Contratistas y Terceros de la Agencia Nacional Digital que requieran enviar o intercambiar información propia de la Entidad, deben hacerlo en las condiciones adecuadas de seguridad sin ponerla en riesgo. Para esto deben, utilizar los canales autorizados, las herramientas tecnológicas de cifrado autorizadas por la Agencia cuando sea requerido para información sensible.

Para el uso de mensajería electrónica se han definido los siguientes lineamientos:

- Se deben proteger los mensajes contra acceso no autorizado a través de mecanismos de control de acceso o cifrado de la información.
- El usuario debe asegurar el transporte de la información al destino correcto validando las direcciones de los correos electrónicos de los destinatarios.
- El Proceso de Gestión de Tecnologías de la Información debe asegurar la disponibilidad y confiabilidad del servicio de correo electrónico a los usuarios.

- Se deben considerar los requisitos legales en términos de transmisión de los datos y autenticidad de los mismos. Para esto, se deben utilizar sistemas de control de accesos y de autenticación.
- Se debe disponer de una autorización de la Agencia para uso de correo electrónico, redes sociales, o cualquier recurso para la transmisión de mensajes.
- El Proceso de Gestión de Tecnologías de la Información debe implementar los sistemas de control de acceso con usuarios y contraseñas fuertes de acuerdo con la *política de control de acceso*.

13.3. Ciberseguridad

La Agencia Nacional Digital protege y asegura la información, sistemas y aplicaciones provenientes y que viajan en el ciberespacio y que son esenciales para la operación de la Agencia, para prevenir, mitigar y disminuir los impactos negativos potenciales de amenazas o ataques cibernéticos, mediante los controles de seguridad, las políticas y los procedimientos de seguridad y privacidad de la información, y el trabajo conjunto con entidades de apoyo en ciberseguridad y ciberdefensa. La gestión de ciberseguridad de la Agencia Nacional Digital contempla las etapas definidas como buenas prácticas del framework de ciberseguridad de la NIST como son la identificación, protección, detección, respuesta y comunicación, recuperación y aprendizaje, las cuales están enfocadas en la adecuada administración de riesgos de ciberseguridad y el mejoramiento continuo de la seguridad digital. Lo anterior se concreta a través del cumplimiento de las siguientes obligaciones:

- El Oficial de Seguridad de la Información debe gestionar eficazmente la ciberseguridad tratada a través de los sistemas informáticos de la Agencia Nacional Digital, así como los activos que participan en sus procesos.

- El Oficial de Seguridad de la Información debe preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con la normatividad vigente en los sistemas de información y comunicación, aplicaciones y servicios de la Agencia Nacional Digital.

- El Oficial de Seguridad de la Información debe promover la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas y la operación de la Agencia Nacional Digital.

- El Oficial de Seguridad de la Información debe analizar los incidentes de ciberseguridad que le son escalados y activar el *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales*, así como contactar a las autoridades y grupos de interés especiales, cuando sea necesario.

- El Oficial de Seguridad de la Información debe realizar las capacitaciones que deben recibir regularmente los Empleados de Planta de la Agencia Nacional Digital en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.

- El Proceso de Gestión de Tecnologías de la Información con el apoyo del Oficial de Seguridad de la Información debe realizar la identificación, análisis y valoración de riesgos cibernéticos para los sistemas de información (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).

- El Oficial de Seguridad de la Información debe proponer los controles para mitigar los riesgos que puedan afectar la seguridad de información confidencial, en reposo o en tránsito.

- El Oficial de Seguridad de la Información debe definir indicadores y medir periódicamente mínimo cada tres (3) meses la eficacia y eficiencia de la gestión de la ciberseguridad.

- El Oficial de Seguridad de la Información cuando sea requerido puede realizar estudios de viabilidad de un presupuesto o póliza de seguro que pueda cubrir costos asociados a posibles ataques cibernéticos. Dichos estudios deben ser presentados con sus recomendaciones al Comité Institucional de Gestión y Desempeño.

- En la Agencia Nacional Digital se deben preservar, cuando sea posible las evidencias digitales para que las autoridades puedan realizar las investigaciones correspondientes.

- El Oficial de Seguridad de la Información debe apoyar el plan de continuidad del negocio para dar respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

- El Proceso de Gestión de Tecnologías de la Información debe mantener actualizados y en operación las herramientas y/o servicios que provee la Agencia Nacional Digital y que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.

- El Proceso de Gestión de Tecnologías de la Información debe monitorear continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la Agencia Nacional Digital.

- En la ADN se debe aplicar el *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales* cuando se presenten ciberincidentes para determinar los elementos de la red que permitan identificar dispositivos que pudieran haber resultado afectados.

- En la Agencia Nacional Digital se deben adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes de un ataque cibernético.

- El Oficial de Seguridad de la Información debe asesorar al Comité de Gestión y Desempeño en temas que considere necesarios sobre ciberseguridad para que puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia.

- El Oficial de Seguridad de la Información debe proponer anualmente los proyectos y/o presupuestos en materia de ciberseguridad en el *plan de seguridad de la información*.

- El Oficial de Seguridad de la Información debe identificar y proponer los controles para la ciberseguridad que impliquen la adopción de nuevas tecnologías.

- El Oficial de Seguridad de la Información debe socializar cuando sea pertinente, las lecciones aprendidas en materia de gestión de ciberincidentes al interior de la Agencia Nacional Digital.

- El Oficial de Seguridad de la Información debe reportar al COLCERT directamente o a través de CSIRT sectoriales, CSIRT de gobierno o CSIRT de la policía, o a quien haga sus veces, los ataques cibernéticos que requieran de su gestión.

13.1.1. Uso de servicios de correo electrónico

La Agencia Nacional Digital debe establecer las reglas generales para asegurar una adecuada protección de la información cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados, a través de los procedimientos asociados.

13.1.2. Uso de servicio de acceso a internet

La Agencia Nacional Digital se asegura una adecuada protección de la información cuando se hace uso del servicio de internet por parte de los usuarios autorizados de la Agencia Nacional Digital, mediante la aplicación de la política de control de acceso y política de seguridad de las comunicaciones.

13.1.3. Servicios de computación en la nube

La Agencia Nacional Digital se debe mantener la seguridad de la información, privacidad de los datos personales y ciberseguridad y de los servicios de procesamiento de información en plataformas de computación en la nube, reduciendo los riesgos legales y técnicos a niveles aceptables.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1. Requisitos de Seguridad de los Sistemas de Información

En la Agencia Nacional Digital con el apoyo del Oficial de Seguridad de la Información y el Proceso de Gestión de Tecnologías de la Información se debe incorporar y validar la seguridad en los sistemas propios y de servicios durante su ciclo de vida de desarrollo del software.

14.1.1. Análisis y Especificación de Requisitos de Seguridad de la Información y Privacidad de los Datos Personales

Todos los desarrollos o software de la Agencia Nacional Digital deben incorporar requisitos de seguridad de la información y privacidad de los datos personales que aseguren la protección de los datos a nivel operacional y de usuario.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con su equipo de trabajo son responsables de definir los requisitos de seguridad de la información y privacidad de los datos personales para todas las aplicaciones o desarrollos propios de la Agencia Nacional Digital de aplicaciones de servicios.

Se deben restringir y controlar el acceso al código fuente del software desarrollado por la Agencia Nacional Digital, solo se otorga el acceso al personal autorizado y se debe llevar control de los cambios autorizados al código fuente.

Los requerimientos como mínimo deben incorporar requisitos de seguridad de la información y privacidad de los datos personales:

- Suministros de acceso autorizados previamente por el propietario o dueño del activo.
- Control de acceso con sistemas de autenticación con usuario y contraseña fuerte.
- Protección de datos personales.
- Informar a los usuarios y operadores sobre las responsabilidades sobre los desarrollos o software.
- Necesidades de protección sobre la disponibilidad, confidencialidad e integridad de la información.
- Registros o logs de auditoría sobre el desarrollo o software.
- Periodos de inactividad.
- Controles de sesiones múltiples.
- Cifrado de la información.
- Sistema de administración de usuarios sobre el desarrollo.

- Otros que se consideren de acuerdo con las necesidades del requerimiento.

14.1.2. Seguridad de Servicios de las Aplicaciones en Redes Públicas

Toda información dispuesta en la operación de la Agencia Nacional Digital de los servicios de aplicaciones que pasan o se ejecutan sobre redes públicas debe ser protegida con medidas de seguridad pertinentes que permitan salvaguardarla de amenazas informáticas que puedan afectar su integridad, disponibilidad y confidencialidad. Para esto el Comité de Seguridad de la Información y Privacidad de los Datos Personales, debe definir los controles necesarios para cumplir a nivel de seguridad técnica, operativa y legal el cumplimiento de dicho propósito.

La seguridad de servicios de aplicaciones sobre redes públicas debe cumplir lo siguiente:

- Sistemas de autenticación que permitan la identidad sobre el uso de la aplicación.
- Procesos de autorización sobre firmas de documentos cuando sea requerido.
- Asegurar que los usuarios de la comunicación estén informados sobre las autorizaciones sobre el uso del servicio.
- Cumplir requisitos de confidencialidad, integridad y disponibilidad de la información.
- Requisitos de integridad para la información de entrada y salida determinada a través de sistemas de autenticación, por ejemplo, con hash.
- Cifrado de la información sobre los canales y sobre el servicio o aplicación.
- Registros o logs de auditoría sobre las transacciones realizadas del servicio sobre la red.
- Responsabilidades civiles establecidas en los acuerdos o convenios sobre el uso del servicio.

14.1.3. Protección de Transacciones de los Servicios de las Aplicaciones

La Agencia Nacional Digital debe proteger la información transaccional de los servicios de las aplicaciones propias y aquellas externas de las cuales asume dicha responsabilidad, con el fin de evitar alteraciones o pérdidas de trazabilidad en el desarrollo de las mismas.

Para las transacciones de los servicios de las aplicaciones deben disponer de los siguientes requisitos de seguridad:

- Uso de firmas electrónicas para las partes que hacen la transacción.
- Sistemas de autenticación con usuario y contraseña.

- Cifrado de la información, de la transacción y del canal utilizado. El Cifrado debe estar dado por una entidad certificadora.
- Registros o logs de auditoría sobre la transacción.

14.2. Seguridad de los Procesos de Desarrollo y Soporte

En la Agencia Nacional Digital se deben incorporar los requisitos de seguridad de la información y privacidad de los datos personales pertinentes durante el ciclo del desarrollo del software o de las aplicaciones.

14.2.1. Política de Desarrollo Seguro

Todo desarrollo de software o aplicación de la Agencia Nacional Digital debe cumplir los requisitos de seguridad de la información y privacidad de los datos personales establecidos por el Oficial de Seguridad de la Información para tal fin.

Para el desarrollo seguro se debe cumplir lo siguiente:

- Seguridad del ambiente de desarrollo con sistemas de autenticación con usuario y contraseña.
- Utilización de codificación segura de acuerdo con el lenguaje de programación utilizado.
- Definición de actividades de verificación dentro de los hitos del proyecto de desarrollo.
- Repositorios seguros del software, protegidos con controles de acceso a través de cifrado de la información o restricciones con usuario y contraseña.
- Control de versión del software, debidamente controlado.
- Análisis de vulnerabilidades del software realizado por el Oficial del Seguridad de la Información, su equipo de trabajo o Empresa Especializada.

14.2.2. Control de Cambios en Sistemas de Información

Los cambios en el software o sistemas de información de la Agencia Nacional Digital durante el ciclo de desarrollo deben ser gestionados conforme al *procedimiento de gestión de cambios* establecido.

14.2.3. Revisión Técnica de las Aplicaciones después de los Cambios en Producción

Todo desarrollo de software debe tener una revisión a nivel técnico, seguridad, funcional y de usuario por los encargados de dichos procesos.

14.2.4. Restricciones en los Cambios en el Software

Las restricciones en los cambios del software y de aplicaciones de la Agencia Nacional Digital deben limitarse a realizar solo las modificaciones o ajustes necesarios, y a su vez, ser monitoreados por los encargados de las revisiones técnicas.

Para el caso del software que requiera cambios o modificaciones se debe:

- Evaluar el riesgo sobre la integridad de la información, los controles aplicados sobre la misma, el cual pueden verse comprometidos, y de manera especial sobre la continuidad del negocio o de las operaciones del servicio prestado o contratado por la Agencia Nacional Digital.

- Disponer del consentimiento o aprobación del propietario del software, sea interno o un proveedor del mismo.

- Notificar los cambios solicitados, y evaluarlos previamente a ser realizados. Dicha evaluación debe ser realizada por Oficial de Seguridad de la Información y el Proceso de Gestión de Tecnologías de la Información.

- Todo cambio en los desarrollos o software debe ser realizado inicialmente sobre el ambiente de pruebas, previo a ser pasado al ambiente de producción.

14.2.5. Principios en la Construcción de Sistemas Seguros

Todo software, aplicación o sistemas de información desarrollado en la Agencia Nacional Digital debe partir de un establecimiento, documentación, principios de diseño seguro, aplicados en su ciclo de vida de su implementación. En cumplimiento de lo anterior, se debe:

- Definir e implementar los requisitos de seguridad de la información y privacidad de los datos personales requeridos para el desarrollo del sistema o software conforme a la necesidad, funcionalidad y operación de la misma. Dichos requisitos deben ser definidos por el Oficial de Seguridad de la Información cuando se requiera el diseño de un software.

- Se deben realizar análisis de riesgos sobre todo requerimiento de software, previamente a ser diseñado. Los riesgos deben ser identificados en conjunto por la Subdirección de Desarrollo, el Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la Información, determinando los controles necesarios para mitigarlos durante su proceso de construcción.

- La Subdirección de Desarrollo con el Oficial de Seguridad de la Información y el Proceso de Gestión de Tecnologías de la Información deben realizar periódicamente (a intervalos definidos previamente), durante el proceso de construcción el cumplimiento de los requisitos establecidos para el mismo.

- Se deben realizar pruebas de seguridad del software (estáticas y dinámicas), a través de análisis de vulnerabilidades sobre los desarrollos por parte del Oficial de Seguridad de la Información de manera interna o externa a través de empresas especializadas, el cual permitan identificar las debilidades sobre el software a ser fortalecidas con controles que mitiguen el impacto de posibles amenazas informáticas al que pueda verse expuesto.

- El Proceso de Gestión de Tecnologías de la Información en sus posibilidades técnicas y competentes es responsable de aplicar los controles necesarios a nivel tecnológico que permitan mitigar las vulnerabilidades técnicas encontradas en los desarrollos. De no ser posible dar solución a las mismas a nivel interno, debe informar al Oficial de Seguridad de la Información la situación, y gestionar una solución alterna, remitiéndola a un Tercero especialista. Dicha posibilidad de transferencia de mitigación de la vulnerabilidad debe ser analizada y aprobada previamente por el Comité de Seguridad de la Información.

14.2.6. Ambiente de Desarrollo Seguro

En la Agencia Nacional Digital se debe disponer de ambientes de desarrollo seguros para llevar acabo los diferentes proyectos de construcción de software, aplicaciones o sistemas de información durante todo el ciclo de vida. Para esto, dichos ambientes deben considerar los siguientes requisitos:

- Evaluarse los riesgos sobre el ambiente de desarrollo frente amenazas informáticas. Para esto a dicho ambiente, se le debe realizar pruebas de seguridad por parte el Oficial de Seguridad de la Información.
- No se debe utilizar información confidencial sensible y original en el ambiente de desarrollo.
- Sistemas de autenticación con usuarios y contraseñas fuertes conforme a los lineamientos de la política de control de acceso de este documento.

- Repositorios seguros del código, restringidos de personal no autorizado. Para el caso de repositorios en la nube o externos, estos deben disponer de controles de seguridad requeridos por la Agencia Nacional Digital, el cual deben cumplir como mínimo los mismos controles que se han determinado para el ambiente de desarrollo externo.
- Disponer de controles de acceso adecuados de acuerdo con las *políticas de control de acceso establecidas*.
- Cualquier cambio en el ambiente de desarrollo, sea físico, en la parte lógica y de usuarios, debe ser aplicado conforme al *procedimiento de gestión de cambios* establecido en la Agencia Nacional Digital. Esto indica, que todo cambio debe tener un estudio y autorización por las partes o encargados pertinentes, previa antes de ser ejecutado.
- Los propietarios o asignados de los ambientes de desarrollo son responsables de:

    - Hacer seguimiento y control sobre los mismos; y de los códigos y datos que se almacenan en sus repositorios.
    - Realizar copias de seguridad sobre la información de códigos y datos que se almacenan en los mismos.
    - Llevar un control del movimiento de información o datos al ambiente de desarrollo.
    - De informar a su Jefe inmediato cualquier incidencia, riesgo o vulnerabilidad identificada en el ambiente.

14.2.7. Desarrollo Contratado Externamente

Todo desarrollo contratado externamente por la Agencia Nacional Digital debe ser monitoreado por la Subdirección de Desarrollo y Supervisores Delegados, con el apoyo del Proceso de Gestión de Tecnologías, el Oficial de Seguridad de la Información y Privacidad de los Datos. Para contratar el desarrollo a entidades externas o proveedores se establecen los siguientes lineamientos:

- La Agencia Nacional Digital con el solicitante, responsable del desarrollo, el Proceso de Gestión de Tecnologías de la Información y el Oficial de Seguridad de la Información deben definir los requerimientos de software en términos de funcionalidad, calidad y seguridad del mismo, y ser acordados previamente con el proveedor.
- Contratos, acuerdos o convenios que definan las cláusulas legales, técnicas, operativas y de seguridad que permitan un desarrollo seguro para la Agencia Nacional Digital.
- Acuerdos de niveles de servicio en el cual se definan prácticas seguras de diseño, codificación y de las pruebas de calidad y seguridad realizadas sobre el software.
- Acuerdos de confidencialidad, acuerdos de licenciamiento, derechos de autor, propiedad intelectual y tratamiento de los datos conforme a las políticas establecidas en la Agencia Nacional Digital.

- Pruebas de seguridad sobre el software realizadas por el proveedor, el cual deben ser solicitadas, validadas y aprobadas por el Supervisor del contrato de la Agencia Nacional Digital.
- El Supervisor del contrato del software debe probar y dar su aceptación a nivel de funcionalidad, calidad y seguridad sobre el mismo para ser puesto en operación en la Agencia Nacional Digital.
- El Supervisor del contrato con el apoyo del Oficial de Seguridad de la Información deben revisar los requisitos de seguridad de la información y privacidad de los datos personales exigidos para el software.
- El Supervisor del contrato del software con el apoyo de la Subdirección Jurídica debe solicitar y validar los certificados de garantía propios del desarrollo del software, especialmente, aquellos requisitos a nivel legal a cumplirse cuando el código fuente no vaya o sea propiedad de la Agencia Nacional Digital.
- Definir en el contrato o ANS, la realización de auditorías por parte de la Agencia Nacional Digital al Proveedor sobre las instalaciones, infraestructura, procesos de desarrollo y la seguridad aplicada donde ejecutan los proyectos de la Agencia Nacional Digital acordados con el Contratista o Tercero.
- El Supervisor del contrato debe solicitar al Proveedor la aplicación y documentación del uso de ambientes de desarrollo, pruebas y producción, así como de todo el software.
- El Supervisor del contrato por parte de la Agencia Nacional Digital es responsable del cumplimiento de todas las medidas legales aplicables en el acuerdo con el Proveedor.

14.2.8. Pruebas de Seguridad de Sistemas

Los desarrollos a nivel interno o externos adquiridos por la Agencia Nacional Digital se les debe realizar pruebas de seguridad y calidad del software conforme a los procedimientos establecidos.

Las pruebas de seguridad de los sistemas deben planearse y documentarse en un plan o programa detallado con sus respectivas actividades, requisitos de entrada y salida; y resultados esperados.

Las pruebas de seguridad de los sistemas deben ser ejecutadas por el Oficial de Seguridad de la Información con el apoyo de la Subdirección de Desarrollo y el Proceso de Gestión de Tecnologías.

Se deben realizar pruebas de seguridad de manera independiente a los desarrollos internos y adquiridos con terceros.

14.2.9. Pruebas de Aceptación de los Sistemas

En la Agencia Nacional Digital para todo sistema, aplicación o software nuevo, actualización o cambios de versión del mismo, se le deben realizar pruebas de aceptación en el cual se valide que cumplen con los resultados esperados, cumpliendo con los requerimientos establecidos.

Las pruebas de aceptación deben realizarse sobre el cumplimiento específico de:

- Requisitos de seguridad de la información y privacidad de los datos personales del software.
- Lineamientos de desarrollo seguro de los sistemas.
- Infraestructura tecnológica que soporta el software.
- Mitigación de vulnerabilidades encontradas del software.

Las pruebas de aceptación deben ser realizadas de manera conjunta por la Subdirección de Desarrollo con el apoyo del Proceso Gestión de Tecnologías, Oficial Seguridad de la Información, el Oficial de Protección de Datos Personales, en un ambiente de pruebas similar al real, de tal manera que se determine y se asegure que son confiables.

14.3. Datos de Prueba

En la Agencia Nacional Digital se deben proteger los datos de las pruebas realizadas a los desarrollos internos o externos adquiridos conforme a las políticas de seguridad que apliquen.

14.3.1. Protección de los Datos de Prueba

Los datos de prueba del software en la Agencia Nacional Digital deben ser seleccionados, protegidos y controlados adecuadamente, y de manera conjunta por la Subdirección de Desarrollo, Gestión de Tecnologías y Seguridad de la Información, y/o sus delegados, que hacen parte de este proceso. Para esto, se debe realizar un análisis previo de uso de los datos de prueba, el cual debe ser autorizado por el Oficial de Seguridad de la Información, dando las pautas de seguridad necesarias para su aplicación y supervisando cuando lo requiera dicho proceso.

No se debe utilizar datos sensibles para realizar pruebas del software o de los sistemas de información.

Para el caso que se requiera definitivamente utilizar datos sensibles, como una excepción, estos deben ser analizados, evaluados y autorizados por el Oficial de Protección de Datos Personales y el Oficial de Seguridad de la Información previamente.

Se debe asegurar la pérdida de confidencialidad de los datos utilizados en las pruebas a través de un protocolo de seguridad que se establezca por los Oficiales de Seguridad y Privacidad de la Información, respectivamente, para su uso.

Todos los datos de prueba utilizados deben ser eliminados de manera segura de los ambientes de prueba. Dicho proceso debe realizarse con las herramientas de borrado seguro autorizados y utilizados en la Agencia Nacional Digital para este propósito.

Con el fin de proteger los datos que se utilicen para pruebas, en la Agencia Nacional Digital se debe cumplir con:

- Controles de acceso para los ambientes de desarrollo y de pruebas.
- Autorización previa por el Oficial de Seguridad de la Información la puesta en operación de los datos de prueba en los diferentes ambientes de desarrollo y pruebas.
- Se debe borrar de manera segura los datos utilizados en los ambientes de desarrollo y pruebas una vez se hayan finalizadas las pruebas o uso en dichos ambientes.
- Toda copia y uso de los datos que se pongan en los ambientes de desarrollo y de pruebas deben ser registrados en un formato o en un log emitido por el sistema donde se deje una trazabilidad de la utilización de los mismos.

15. RELACIONES CON LOS PROVEEDORES

15.1. Seguridad de la Información y Privacidad de los Datos Personales en las Relaciones con los Proveedores

En la Agencia Nacional Digital se deben proteger los activos de la información que se comparten o intercambian de manera autorizada con los proveedores.

15.1.1. Políticas de Seguridad de la Información y Privacidad de los Datos Personales para las Relaciones con Proveedores

La Agencia Nacional Digital se deben proteger los activos que sean accesibles a los proveedores a través del cumplimiento de las siguientes obligaciones generales:

Obligaciones:

1. En la Agencia Nacional Digital en caso de requerir o prestar un servicio, producto o intercambio de información con un tercero, establecerá contratos, acuerdos o convenios.

2. Los contratos, acuerdos o convenios con terceros se deben desarrollar con la identificación de las necesidades de negocio, el análisis costo beneficio, tener acuerdos de nivel de servicio (ANS), que incluyan los requisitos de seguridad y cumplimiento de la Política de Seguridad de la Información y Privacidad de los Datos Personales.

3. Los contratistas requeridos para prestar servicios propios de funciones de roles o cargos de su estructura organizacional de la Agencia Nacional Digital deben ser seleccionados con el apoyo de la Subdirección Administrativa y Financiera, de acuerdo con el *procedimiento de selección de personal* y siguiendo el *procedimiento de contratación* aplicado por la Subdirección Jurídica.

4. Para el caso que se requiera establecer intercambios de información con terceros en beneficio o compartido o propio de sus servicios u operaciones, debe definir y aprobar acuerdos o convenios con el tercero con las debidas cláusulas legales, requisitos seguridad de la información y privacidad de datos personales.

5. Todo tipo de contrato, acuerdo o convenio debe estar autorizado por la Dirección de la AND y tener un Supervisor asignado, responsable y encargado de llevar a cabalidad la ejecución

6. Para la selección de un proveedor, cada Líder de Proceso o Supervisor asignado debe realizar verificaciones de antecedentes de dichos proveedores y, en caso de que sea necesario, se deben determinar los métodos que deben aplicarse para la verificación de éstos.

7. 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 Agencia Nacional Digital auditar el cumplimiento de las políticas por parte de los proveedores, asegurando que el personal autorizado de la Agencia pueda evaluar dicho cumplimiento.

8. El Oficial de Seguridad de la Información y los responsables de la contratación, deben identificar los riesgos de seguridad relacionados con proveedores durante el proceso de evaluación de riesgos, teniendo en cuenta la criticidad de la información, y de acuerdo con la metodología de evaluación y tratamiento de riesgos de la Agencia Nacional Digital. Durante la evaluación de riesgos, se debe tener especial cuidado para identificar riesgos relacionados con tecnologías de la información y comunicación, como también riesgos relacionados con la cadena de suministro de productos.

9. El Supervisor del contrato debe exigir al proveedor que disponga de un acuerdo o declaración de confidencialidad con sus empleados que se encuentren asignados para desarrollar las actividades de la Agencia Nacional Digital.

10. Todos los incidentes de seguridad relacionados con la ejecución del contrato con el proveedor deben ser reportados por el supervisor del contrato por medio del *procedimiento de notificación y gestión de incidentes de seguridad de la información y privacidad de los datos personales*.

11. En caso de que se modifique o finalice un contrato, se deben eliminar los derechos de acceso para los empleados del proveedor, de acuerdo con la *Política de Control de Acceso a la Información y Privacidad de los Datos Personales* descrita en este documento. Así mismo, el Supervisor del contrato debe asegurarse que todo el equipamiento, software e información que se encuentre en medios de almacenamiento propios de la Agencia Nacional Digital sean devueltos. Así mismo, debe asegurarse de obtener toda la información electrónica de la ejecución del contrato por medio de copias o backups, en los medios que sean acordados entre las partes. Dichas copias deben ser verificadas por parte del Supervisor del contrato y una vez validadas, debe exigir al proveedor que elimine de manera segura toda la información de la Agencia Nacional Digital relacionada con el contrato conforme a los requisitos dados en el mismo.

12. Todos los Supervisores que tienen bajo su responsabilidad un contrato con Proveedores deben seguir el *procedimiento de seguridad de terceros* para realizar la gestión del mismo.

La Agencia Nacional Digital debe exigir requisitos a los terceros, como los siguientes:

- Identificación y documentación del tipo de tercero (Contratistas, Proveedor, otro).
- Registro como proveedor con la Agencia Nacional Digital.
- Tipos de acceso a la información.
- Requisitos mínimos de seguridad de la información.
- Procedimientos de seguimiento al cumplimiento de los requisitos de seguridad de la información.
- Controles de confidencialidad, integridad, disponibilidad y privacidad de la información.
- Obligaciones aplicables al tercero respecto a la protección de la información a través de acuerdos de confidencialidad.
- Manejo de incidentes y continuidad de los servicios.
- Control de cambios.
- Planes de continuidad del negocio.
- Formación y concienciación de seguridad de la información del equipo de trabajo.
- Acuerdos de confidencialidad del equipo de trabajo.
- Acuerdo o contrato de requisitos de seguridad de la información firmado con el Tercero. Este puede estar incluido en el ANS.
- Acuerdo de transmisión o intercambio de información.
- Políticas de seguridad de la información.

- Demás requisitos exigidos por la Agencia…

15.1.2. Tratamiento de la Seguridad en los Acuerdos con los Proveedores

En la Agencia Nacional Digital se deben acordar los requisitos de seguridad de la información y privacidad de los datos personales con los proveedores conforme a las políticas de seguridad establecidas, el objeto contractual y al tratamiento de la información requerida para llevar acabo los servicios contratados. Así, los responsables de la contratación de proveedores deben establecer y acordar: la información a tratar; niveles de clasificación, finalidad del tratamiento de la información personal que está autorizado para el tratamiento de la información; controles para tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor. Se definen los siguientes lineamientos en cumplimiento de requisitos de seguridad de la información:

- Se debe realizar una definición de la información que se va a suministrar y compartir con el Tercero, así como los medios, por los cuales se va a intercambiar o transmitir.
- Clasificación de la información que se comparte con el Tercero, comparando el tipo de clasificación que utiliza el mismo.
- Requisitos legales y contractuales sobre propiedad de la información, derechos de autor y propiedad intelectual, protección de datos personales, y la forma en que se acuerda el cumplimiento de los mismos.
- Controles de acceso sobre la información, derechos de auditoría y revisiones de desempeño.
- Reglas de aceptación de la información.
- Listado de personal autorizado para el acceso a la información, con sus respectivos datos de contacto.
- Políticas de seguridad de la información fundamentadas en la norma ISO 27001:2013.
- Procedimientos de gestión de incidentes.
- Planes de continuidad del negocio.
- Reglamentación para la contratación externa.
- Formación y conciencia de seguridad de la información de los empleados.
- Modelo contrato de los empleados de tercero donde se evidencien requisitos de seguridad de la información.
- Hojas de vida de personal que emplea el Tercero para prestar el servicio a la Agencia Nacional Digital.
- Procedimiento de solución de problemas o conflictos.
- Derecho de auditar al Tercero.
- Informes de seguimiento.
- Obligaciones del cumplimiento del Tercero sobre la seguridad de la información.

- Otros que apliquen según sea el caso, el cual deben ser definidos por el Oficial de Seguridad de la Información.

15.1.3. Cadena de Suministro de Tecnología de la Información y Comunicación

En los acuerdos con los proveedores que realice la Agencia Nacional Digital se deben incorporar riesgos de seguridad de la información y privacidad de los datos personales propiamente con el suministro de productos servicios de tecnología y comunicación entre las partes. Se establecen los siguientes lineamientos:

- Se deben acordar los requisitos de seguridad de la información para las adquisiciones de herramientas tecnológicas o servicios con el Tercero.
- Requisitos de seguridad de la información sobre la cadena de suministro, en caso de que el Tercero contrate a otro Tercero para soportar el servicio contratado con la Agencia Nacional Digital.
- Exigir al Tercero la divulgación de prácticas de seguridad de la información a lo largo de la cadena de suministro, en el caso que adquieran elementos tecnológicos comprados a otros proveedores.
- Acordar un procedimientos y métodos de aceptación sobre los productos y servicios de tecnología y comunicaciones.
- Acordar procedimiento de identificación de componentes críticos, especialmente si los mismos son comprados por el Tercero a otro proveedor.
- Solicitar requisitos de seguridad sobre los componentes críticos.
- Solicitar la realización de pruebas sobre el funcionamiento adecuado de los productos o servicios.
- Definir las reglas para compartir información, y solucionar cualquier problema que pueda presentarse.
- Implementar procesos de ciclo de vida y disponibilidad de componentes tecnológicos.
- Evaluar los riesgos sobre el suministro de componentes o servicios proveídos por el Tercero.

15.2. Gestión de la Prestación de Servicios de Proveedores

La Agencia Nacional Digital debe mantener los acuerdos de niveles de servicio establecidos con los proveedores, el cual indiquen los procedimientos, comunicaciones, seguimientos, entre otros, que se consideren necesarios para llevar a cabo la ejecución del contrato. Así mismo, se deben incluir la aceptación de los acuerdos de seguridad en controles y políticas de seguridad y privacidad de la información de la Agencia Nacional Digital, para proteger la confidencialidad, integridad y disponibilidad de los datos y equipos.

15.2.1. Seguimiento y Revisión de Servicios de los Proveedores

Todo Supervisor de contrato de proveedores de servicio de la Agencia Nacional Digital es responsable del seguimiento, revisión, control y monitoreo del mismo. De igual manera, debe reportar al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales cualquier incidente de seguridad de la información y privacidad de los datos personales o riesgo presente en el desarrollo del servicio.

El Supervisor del contrato del proveedor debe revisar y controlar periódicamente el nivel de los servicios, cumplimiento de las cláusulas de seguridad por parte de los proveedores, los informes y registros generados por ellos, y realizar una auditoría al menos una vez al año.

Se debe hacer seguimiento al nivel de desempeño del servicio conforme a lo establecido en los acuerdos.

Se deben revisar los reportes del servicio entregados por el proveedor y programar reuniones de seguimiento periódico.

Se deben llevar auditorías al proveedor de servicios con el apoyo de Control Interno y Líderes de Proceso relacionados al contrato.

Se debe revisar la gestión de los incidentes y problemas resueltos del servicio.

Se debe revisar los aspectos de seguridad de la información del Tercero con sus proveedores que implican directamente el servicio contratado por la Agencia.

Se debe revisar los registros o logs de auditoría generados por el servicio del Tercero.

Se debe asegurar mediante monitoreo, la capacidad de prestación del servicio del Tercero.

15.2.2. Gestión de Cambios en los Servicios de los Proveedores

Cualquier cambio en los servicios o ejecución de los mismos dentro del contrato o en los ANS contratados por la Agencia Nacional Digital deben ser gestionados de acuerdo con el *procedimiento de gestión de cambios* acordado con el proveedor.

Se deben gestionar los cambios en los servicios con los Terceros considerando:

- Los cambios en los acuerdos con el Tercero.

- Los cambios realizados por la Agencia Nacional Digital como mejoras al servicio, desarrollo de nuevas aplicaciones, modificaciones y actualizaciones a políticas y procedimientos, controles nuevos o modificación de los mismos para solución de incidentes.
- Los cambios en los servicios de los Terceros para realizar cambios y mejoras en las redes, uso de nuevas tecnologías, nuevos productos o actualizaciones de los mismos, ambientes de desarrollo optimizados, cambio de ubicación física, cambio o contratación externa de otros proveedores o Terceros.

Cuando se realizan modificaciones o se finaliza el contrato de servicios del proveedor, el Supervisor del contrato es quien comunica sobre las modificaciones o finalización del contrato a la Subdirección Jurídica. El Supervisor del contrato debe realizar una nueva evaluación de riesgos antes de aceptar las modificaciones del contrato.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES

16.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información y Privacidad de los Datos Personales

En la Agencia Nacional Digital se deben gestionar los incidentes de seguridad de la información y privacidad de los datos personales de manera coherente y eficaz, fomentando una comunicación efectiva de los eventos de seguridad y debilidades o vulnerabilidades detectadas sobre los activos de información y su apropiada gestión, implementando las acciones correctivas y oportunidades de mejora correspondientes.

16.1.1. Responsabilidades y Procedimientos

En la Agencia Nacional Digital frente a la gestión de incidentes de seguridad de la información y privacidad de los datos personales, se establecen las siguientes responsabilidades y procedimientos con el fin de generar acciones de control para asegurar una respuesta rápida, efectiva, eficaz y organizada:

El Oficial de Seguridad de la Información es responsable de gestionar los incidentes de seguridad de la información de la Agencia Nacional Digital.

Los Líderes de Proceso son responsables de atender los incidentes de seguridad de la información propios de su proceso con el apoyo del Oficial de Seguridad de la Información.

La gestión de incidentes en la Agencia Nacional Digital debe contemplar actividades de seguimiento, detección, análisis, reporte y respuesta a los mismos.

Los incidentes de seguridad de la información deben ser registrados con el fin de llevar un control sobre su gestión.

La gestión de incidentes debe disponer de una clasificación y valoración de los mismos para la toma de decisiones.

La respuesta de incidentes debe partir de una clasificación y escalado por niveles de atención conforme a las competencias de los procesos de la Agencia y personal capacitado.

Se debe realizar seguimiento a los incidentes de seguridad de la información.

La gestión de incidentes debe disponer de personal competente para dar respuesta a los mismos.

En la Agencia Nacional Digital se debe disponer de un punto de contacto para el reporte y atención de los incidentes de seguridad de la información.

Se debe mantener contacto y un inventario actualizado de contacto con las autoridades civiles, militares, legales, de servicios y demás grupos de interés para dar respuesta a los incidentes de seguridad de la información según sea el caso.

El reporte de los incidentes de disponer de un formato o registro para los mismos, las actividades a seguir, la referencia a un control disciplinario formal, y procesos de retro alimentación que permitan ser notificados frente a la respuesta de los mismos.

La gestión de incidentes se debe planificar con el fin de establecer respuesta a los mismos.

La atención de los incidentes en la Agencia Nacional Digital puede tener un tratamiento externo de acuerdo con la situación dada, en caso de que no se disponga de los recursos o capacidades técnicas para resolverlo internamente. Dicho traslado del tratamiento del mismo debe ser previamente autorizado conforme al procedimiento establecido.

16.1.2. Reporte de Eventos de Seguridad de la Información y Privacidad de los Datos Personales

Todos los trabajadores, Contratistas y proveedores que tienen acceso a los activos de información de la Agencia Nacional Digital, deben reportar a través de los canales dispuestos por ésta, de acuerdo con el

procedimiento de notificación y gestión de incidentes de seguridad de la información y privacidad de los datos personales dispuesto en la carpeta compartida de la Agencia Nacional Digital-Modelo de Gestión, cualquier situación que se pueda considerar como un incidente o amenaza de seguridad que comprometa o afecte las operaciones y servicios.

Las eventualidades que deben considerar el reporte de incidentes de seguridad de la información en la Agencia son las siguientes:

- Deficiencia en los controles de seguridad.
- Vulneración de los principios de seguridad (confidencialidad, integridad y disponibilidad) y a la privacidad de la información.
- Fallas humanas o errores involuntarios.
- No conformidades de políticas o procedimientos.
- Violaciones a la seguridad física o lógica.
- Cambios no contralados o no autorizados en los sistemas.
- Fallas en software o hardware.
- Intentos o accesos no autorizados a los sistemas de información.
- Otras que afecten la seguridad de la información de la Agencia.

16.1.3. Reporte de Debilidades de Seguridad de la Información y Privacidad de los Datos Personales

Aquellas actividades que generen sospecha de un evento que comprometa la Seguridad de la Información y Privacidad de los Datos Personales de la Agencia Nacional Digital, deben ser registradas en los formatos asociados al *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales de* forma que puedan ser usadas como evidencia en la aplicación de acciones correctivas acordes con el impacto causado en caso de que se materialice.

Es responsabilidad y obligación de todos los trabajadores, Contratistas y proveedores que tienen acceso a los activos de información de la Agencia Nacional Digital aplicar a cabalidad la *Política de Seguridad de la Información y Privacidad de los Datos Personales*, proteger los activos de información y reportar oportunamente los incidentes de seguridad que se presenten; así como, participar o contribuir con la aplicación de las medidas de mitigación y planes de mejoramiento que se definan para su superación.

Es responsabilidad del Oficial de Seguridad de la información o quien haga sus veces en la Agencia Nacional Digital, presentar al Comité de Gestión y Desempeño un consolidado de los eventos e incidentes reportados y las acciones ejecutadas trimestralmente, en función de los controles

establecidos en la implementación de la Política de Seguridad y Privacidad de la Información, así como las recomendaciones y planes de acción para la mitigación de incidentes.

Se deben definir planes de uso y apropiación para los trabajadores y Contratistas de la Agencia Nacional Digital, relacionados con la identificación de incidentes de seguridad sobre los activos de información de la Agencia Nacional Digital y la forma de reportarlos y resolverlos.

Se debe hacer el reporte de incidentes en caso de que afecten datos personales a la Profesional Jurídica u oficial de datos personales o quien haga sus veces, enviando el *Formato Reporte de incidentes de seguridad* diligenciado con la información.

La Agencia Nacional Digital debe contar con protocolos de comunicación sobre los incidentes de seguridad como el *Procedimiento para Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales.*

El *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales* de la Agencia Nacional Digital debe ser implementado en caso de identificación de incidentes.

16.1.4. Evaluación de Eventos de Seguridad de la Información y Privacidad de los Datos Personales y Toma de Decisiones

Los eventos o incidentes de seguridad de la información y privacidad de los datos personales en la Agencia Nacional Digital se deben evaluar y tomar decisiones sobre los mismos conforme al *Procedimiento para Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales*.

La evaluación de los eventos de seguridad y privacidad de la información deben ser evaluados conforme a su clasificación establecida en el procedimiento definido.

16.1.5. Respuesta a Incidentes de Seguridad de la Información y Privacidad de los Datos Personales

La Agencia Nacional Digital debe dar respuesta a los incidentes de seguridad de la información y privacidad de los datos personales de acuerdo con lo establecido en el *Procedimiento para Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales*.

Las respuestas a los incidentes de seguridad de la información deben incluir:

- La recolección de las evidencias.

- Un análisis forense de seguridad de la información.
- Un escalamiento de niveles de atención sobre el mismo.
- Un registro de las actividades realizadas como respuesta al incidente.
- Una comunicación formal del incidente a los usuarios que lo han reportado, responsables y afectados directos.
- Un tratamiento del incidente mediante la aplicación de controles pertinentes.
- Un cierre y un registro del mismo al ser solucionado.

Se debe realizar un análisis posterior a nivel de retest de validación de aplicación de controles adecuadas para la atención del incidente.

16.1.6. Lecciones Aprendidas de los Incidentes de Seguridad de la Información

Es deber del Oficial de Seguridad de la Información en la Agencia Nacional Digital comunicar los incidentes de seguridad de la información y privacidad de los datos personales y respuesta a los mismos, al personal que aplique, como aprendizaje y mejora continua en el desarrollo de las operaciones.
Los incidentes deben ser cuantificados frente a los tipos, volúmenes, costos y tratamiento, con el fin de identificar su recurrencia y el nivel de impacto. Esto puede ser un insumo, que indica la efectividad de los controles y posibles revisiones a las políticas de seguridad de la información.

Las situaciones presentadas en los incidentes deben ser utilizadas para generar conciencia a los Empleados de Planta, Contratistas y Terceros en la Agencia Nacional Digital. Para esto se comunicarán a los usuarios pertinentes las lecciones aprendidas que puedan surgir en su ámbito laboral.

16.1.7. Recolección de la Evidencia

En la Agencia Nacional Digital se deben recolectar, analizar y preservar las evidencias de los incidentes de seguridad de la información y privacidad de los datos personales de acuerdo con el *Procedimiento para Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales.*

La recolección de las evidencias de los incidentes de seguridad y privacidad de la información deben cumplir con los siguientes lineamientos mínimos:

- Se debe dar una custodia segura de las evidencias, restringidas de personal no autorizado sobre las mismas.
- Se debe considerar la seguridad del personal que ha participado en la recolección de las evidencias.

- Se deben definir roles y responsabilidades del personal involucrado en el tratamiento de las evidencias.
- Se debe disponer de personal con las competencias necesarias para dar tratamiento adecuado y seguro a las evidencias.
- Se deben documentar el tratamiento de las evidencias en todo su ciclo durante el incidente.
- Se deben realizar sesiones informativas privadas con las personas involucradas que permitan tener un conocimiento más preciso sobre las evidencias presentes en el caso del incidente, y así mismo sobre el tratamiento de las mismas a las personas responsables de dicha función.

Cualquier alteración o manipulación indebida o sin autorización de las evidencias puede ser considerada una falta, el cual puede incurrir en sanciones de acuerdo con lo establecido en el manual interno de trabajo o en lo que la ley aplique.

Las evidencias de los incidentes de seguridad de la información pueden trascender a instancias legales que hacen parte de las competencias de Autoridades Civiles o Judiciales externas a la Agencia, como parte de investigaciones propias de estas Entidades de Control.

17. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

17.1. Continuidad de la Seguridad de la Información

En la Agencia Nacional Digital se debe incluir la seguridad de la información y privacidad de los datos personales en la gestión de la continuidad del negocio el cual conlleven a la preservación de los principios de seguridad (confidencialidad, integridad y disponibilidad), en caso de situaciones adversas que pongan el riesgo la normalidad de las operaciones.

17.1.1. Planificación de la Continuidad de la Seguridad de la Información y Privacidad de los Datos Personales

En la Agencia Nacional Digital el Oficial de Seguridad de la Información con el Oficial de Protección de Datos Personales y los Líderes de Proceso deben planificar la continuidad de la seguridad de la información y privacidad de los datos personales determinando los requisitos pertinentes el cual permitan proteger los activos de información frente a un evento adverso que pueda poner en riesgo las operaciones durante una crisis o desastre.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales debe definir y gestionar la implementación de los requisitos de seguridad de la información y privacidad de los datos personales en la planeación y ejecución del proceso de gestión de continuidad del negocio, considerando

el BIA, Planes de Contingencia, Plan de Recuperación de Desastres, Plan de Emergencias y demás elementos definidos para llevar a cabo este proceso en la Agencia Nacional Digital.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben planificar la seguridad de la información y privacidad de los datos personales en la continuidad del negocio manteniendo una condición normal de los requisitos de seguridad en las operaciones de la Agencia Nacional Digital en una contingencia.

El Oficial de Seguridad de la Información con el Oficial de Protección de Datos Personales y los Líderes de Proceso deben definir los requisitos de seguridad de la información y privacidad de los datos personales para la continuidad a partir de un análisis de impacto del negocio (BIA), identificando los controles necesarios a aplicar frente a posibles escenarios de contingencia o situaciones adversas.

17.1.2. Implementación de la Continuidad de la Seguridad de la Información y Privacidad de los Datos Personales

En la Agencia Nacional Digital se deben mantener documentados, implementados, y con el debido mantenimiento los planes, procesos, procedimientos y controles que permitan asegurar la continuidad de las operaciones y de la seguridad de la información y privacidad de los datos personales en caso de eventos adversos relacionados con cualquier falla o afectación física o lógica de los activos de información.

En la Agencia Nacional Digital se debe establecer una estructura de gestión de continuidad del negocio conformada con personal con las competencias necesarias para responder frente a posibles eventos adversos de crisis. Esta estructura debe estar definida en el *Plan de Continuidad del Negocio* de la ADN.

La gestión de la continuidad del negocio de la Agencia Nacional Digital debe involucrar personal de respuesta a incidentes que permitan apoyar la atención y solución a los mismos.

En la Agencia Nacional Digital se deben definir, documentar y aprobar todos los planes, procedimientos de respuesta y recuperación en los procesos críticos que permitan gestionar la continuidad de las operaciones frente a eventos adversos.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben definir, documentar y gestionar los controles de compensación de seguridad de la información y privacidad de los datos personales que no se puedan mantener a causa de situaciones adversas, el cual permitan mantener un nivel aceptable de la seguridad en dadas en condiciones de contingencia.

17.1.3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información y Privacidad de los Datos Personales

Cada Líder de Proceso en la Agencia Nacional Digital con el apoyo del Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales se debe verificar, revisar y evaluar a través de pruebas o simulacros los planes de continuidad y controles de seguridad de la información y privacidad de los datos personales implementados propios de su proceso para asegurar la efectividad de los mismos frente a situaciones adversas que puedan poner en riesgo el desarrollo normal de las operaciones.

Cualquier cambio requerido en el plan de continuidad del negocio o de sus elementos, deben ser realizados de acuerdo con el *procedimiento de gestión de cambios* de la Agencia Nacional Digital y evaluados frente al cumplimiento de los requisitos de seguridad de la información y privacidad de los datos personales por el Oficial de Seguridad de la Información.

En la Agencia Nacional Digital se deben realizar pruebas de continuidad donde se involucren los procesos, procedimientos y controles de seguridad de la información y privacidad de los datos personales en la continuidad del negocio, con el fin de validar la efectividad de los mismos y el desempeño sobre los objetivos de continuidad frente a situaciones de emergencia y/o contingencia.

En la Agencia Nacional Digital se deben realizar mínimo dos (2) pruebas de continuidad del negocio a los procesos críticos de acuerdo con lo establecido en el plan de continuidad del negocio, o cuando sea requerido por necesidad propia de las operaciones.

Todo cambio realizado al plan de continuidad del negocio de la Agencia Nacional Digital, o a cualquiera de los elementos debe ser probado nuevamente, con el fin de validar la efectividad y desempeño del mismo en condiciones críticas.

En la Agencia Nacional Digital se deben verificar de manera integrada los controles de continuidad del negocio de seguridad de la información y privacidad de los datos personales junto con las pruebas de continuidad del negocio y recuperación de desastres.

17.2. Redundancias

En la Agencia Nacional Digital se debe asegurar la disponibilidad de los recursos físicos y tecnológicos alternos para la continuidad de las operaciones frente eventos adversos.

17.2.1. Disponibilidad de Instalaciones de Procesamiento de la Información

La Agencia Nacional Digital debe disponer de infraestructura física y tecnológica redundante a través de la disposición de canales alternos de comunicación, copias de seguridad actualizadas y probadas, e instalaciones físicas alternas para llevar a cabo sus operaciones en contingencia manteniendo el desarrollo normal de sus operaciones.

El Proceso de Gestión de Tecnologías de la Información debe identificar y gestionar la disponibilidad de recursos tecnológicos necesarios que permitan a la Agencia mantener la infraestructura alterna para llevar a cabo la continuidad de las operaciones de los procesos críticos cuando sea requerido.

El Proceso de Gestión de Tecnologías de la Información debe realizar pruebas a los sistemas y redes de comunicación principales y redundantes de manera preventiva a través de simulacros mínimo dos (2) veces al año y de manera correctiva una vez se haya superado una situación de crisis o contingencia, con el fin de validar su funcionamiento normal de los mismos de acuerdo con los lineamientos del *Plan de Recuperación de Desastres (DRP)*.

La Subdirección Administrativa y Financiera debe identificar y gestionar la disponibilidad de recursos físicos y administrativos necesarios relacionados para la continuidad del negocio.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben evaluar los riesgos de seguridad de la información y privacidad de los datos personales a los activos de información principales y redundantes que actúan frente a la continuidad del negocio de la Agencia Nacional Digital.

18. CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

18.1. Cumplimiento de Requisitos Legales y Contractuales

La Agencia Nacional Digital debe cumplir con los requisitos legales, estatutarios, contractuales y normativos de seguridad de la información y privacidad de los datos personales que apliquen en el desarrollo de sus funciones.

18.1.1. Identificación de la Legislación y Requisitos Contractuales de Seguridad de la Información y Privacidad de los Datos Personales

En la Agencia Nacional Digital el Oficial de Seguridad de la Información con el apoyo del Oficial de Protección de Datos Personales y de la Subdirección Jurídica deben identificar, mantener y trabajar por

dar cumplimiento oportuno y eficaz de la legislación y requisitos contractuales vigentes en materia de seguridad de la información y privacidad de los datos personales. Así mismo, si se contrae o tiene relaciones en otros países debe identificar las regulaciones pertinentes con los mismos conforme al cumplimiento de las mismas y a las buenas prácticas de seguridad y privacidad de la información.

18.1.2. Derechos de Autor y Propiedad Intelectual

En la Agencia Nacional Digital se debe asegurar el cumplimiento de los derechos de autor y propiedad intelectual sobre la información y del software de acuerdo con los requisitos legales vigentes establecidos en la Ley 23 de 1982 "por la cual se regulan los derechos morales y patrimoniales que la Ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística o científica, esté publicada o inédita".

En la Agencia Nacional Digital se debe adquirir el software solo con proveedores reconocidos en el mercado, que garanticen el licenciamiento de los mismos. De esta manera, el Proceso de Gestión de Tecnologías de la Información es responsable de hacer la validación pertinente del proveedor de tecnología y del licenciamiento del software.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con el apoyo del Proceso de Gestión de Tecnologías de la Información y la Subdirección Jurídica debe sensibilizar al personal sobre el uso del software, y en especial sobre el licenciamiento, de tal manera que reconozca a sí mismo las implicaciones legales en caso de cualquier incumplimiento.

El Proceso de Gestión de Tecnologías de la Información es responsable de mantener actualizado el inventario de software con sus respectivas licencias sobre el mismo.

El Proceso de Gestión de Tecnologías de la Información debe controlar el uso de las licencias del software de acuerdo con las necesidades establecidas y la cantidad adquirida.

Las licencias del software solo pueden ser activadas por el Proceso de Gestión de Tecnologías de la Información o su delegado.

El Proceso de Gestión de Tecnologías de la Información y su equipo de trabajo deben realizar revisiones periódicas mínimo una vez al mes del software instalado en los equipos de la Agencia Nacional Digital, con el fin de validar que el software es el autorizado y con el licenciamiento adecuado. Cualquier software identificado que no sea autorizado o no tenga licenciamiento debe ser retirado de inmediato de los equipos y notificada dicha novedad como un incidente de acuerdo con el *procedimiento de notificación y gestión de incidentes de seguridad y privacidad de la información*.

El Proceso de Gestión de Tecnologías de la Información puede utilizar herramientas tecnológicas autorizadas por Comité de Seguridad de la Información y Privacidad de los Datos Personales y realizar la configuración necesaria para controlar la instalación de software no autorizado o no licenciado en los equipos de la Agencia.

El Proceso de Gestión de Tecnologías de la Información previamente a adquirir el software debe revisar los términos y condiciones del mismo, validando que es de beneficio para la Agencia Nacional Digital y que no implicará un riesgo legal u operativo para la Entidad.

En la Agencia Nacional Digital se prohíbe copiar total o parcialmente software, documentos o cualquier información de propiedad de la Agencia Nacional Digital, de su encargo de tratamiento, o de Terceros propietarios de sus derechos de autor, a no ser que sea permitido por parte de dichos derechos y sea autorizado por el propietario o responsable de la misma.

La Agencia Nacional Digital se deben 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 genere, notificando y dejando claro a todos los usuarios dicha propiedad en los diferentes contratos o convenios establecidos. Este lineamiento es responsabilidad de los Líderes de Proceso y la Subdirección Jurídica de la Agencia.

En la Agencia Nacional Digital una vez definido el licenciamiento del software se debe establecer un inventario de software autorizado, el cual debe ser comunicado a todos los usuarios por el Oficial de Seguridad de la Información.

Cualquier incumplimiento de los derechos de autor y propiedad intelectual de cualquier información o producto utilizado puede llevar a penalizaciones o sanciones pertinentes de acuerdo con la legislación nacional o internacional, y a la normatividad interna establecida o aplicada por la Agencia Nacional Digital.

18.1.3. Protección de Registros

En la Agencia Nacional Digital se deben proteger 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.

Los registros deben ser clasificados en la Agencia Nacional Digital de acuerdo con los lineamientos de gestión de activos de la información dados en la presente *Política de Seguridad de la Información y Privacidad de los Datos Personales* y al programa de gestión documental, dados los tiempos de

retención, tipo de almacenamiento, controles de seguridad y demás elementos propios de este sistema de gestión.

Una vez clasificados y dada la criticidad de los registros se debe establecer los controles de acceso y protección necesaria a nivel físico o electrónico, a través de mecanismos de seguridad física o cifrado de la información de acuerdo con lo establecido en la presente política.

El Proceso de Gestión Documental con el Proceso de Gestión de Tecnologías de la Información, el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben determinar los medios de almacenamiento de los registros de manera que los datos se puedan recuperar en tiempos y formatos aceptables de acuerdo con los requisitos legales o de buenas prácticas vigentes aplicables a la Agencia Nacional Digital, y así mismo, validar su deterioro de los mismos o de cambios futuros de tecnología de manera anticipada, con el fin de tomar las medidas previas pertinentes para la migración de la información a otros medios.

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 Agencia Nacional Digital, la información debe ser retirada y destruido dichos medios de manera segura de acuerdo con el *procedimiento de borrado seguro de la información y procedimiento de eliminación segura de medios.*

El Proceso de Gestión Documental junto con cada Líder de Proceso es responsable de definir los lineamientos de retención, almacenamiento, manejo y disposición de los registros. Así como de elaborar el programa de gestión documental y llevar un inventario de la información de todos los procesos.

Los tiempos de retención, medios de almacenamiento, y tratamiento de los registros de la Agencia Nacional Digital de propiedad, responsabilidad o encargo, deben ser establecidos de acuerdo con la legislación vigente aplicable.

La Agencia Nacional debe 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 debe dar el procedimiento frente a la disposición de los registros conservando el cumplimiento legal de la Agencia Nacional Digital y la protección de los datos.

Cuando sea requerido entregar registros por orden judicial, la Agencia Nacional Digital debe realizar dicha entrega conservando la protección de la misma de acuerdo con las *políticas de seguridad de la información y privacidad de los datos personales* establecidas y acordadas con el ente judicial.

18.1.4. Privacidad y Protección de Información de Datos Personales

En la Agencia Nacional Digital se debe asegurar el tratamiento, privacidad y protección de la información de los datos personales conforme a lo establecido en la *política de tratamiento de datos personales de la Agencia Nacional Digital* en cumplimiento de la Ley 1581 de 2012 por la cual se reglamenta la protección de los datos personales en Colombia; y a la *política de seguridad de la información y privacidad de la información de la Agencia Nacional Digital*.

En la Agencia Nacional Digital se ha dispuesto el Oficial de Protección de Datos Personales, en el cual se delega la responsabilidad de asegurar el cumplimiento de la Ley 1581 de 2012.

La Agencia Nacional Digital debe establecer las políticas de tratamiento de datos personales, procedimientos, formatos, y demás elementos, el cual regulen el tratamiento de los datos personales en cumplimiento de la Ley 1581 de 2012. Responsabilidad que asume el Oficial de Protección de Datos Personales.

En la Agencia Nacional Digital debe comunicar las *políticas de tratamiento de datos personales* a través de medios de comunicación, a todos los Empleados de Planta, Contratistas, Terceros, Proveedores, Clientes y público en general.

En la Agencia Nacional Digital debe orientar a la Alta Dirección, Líderes de Proceso, Empleados de Planta, Contratistas, Proveedores, Clientes y toda parte interesada de la Agencia Nacional Digital sobre el tratamiento de los datos personales conforme a su rol, función y contexto sobre la misma. Para esto, debe realizar sensibilizaciones, capacitaciones o campañas de comunicación que permitan tomar conciencia sobre su función sobre las *políticas de tratamiento de datos personales*.

El Oficial de Protección de Datos Personales con el apoyo del Oficial de Seguridad de la Información y el Proceso Gestión de Tecnologías de la Información debe gestionar la implementación de los controles tecnológicos y de seguridad para proteger la información de datos personales.

18.1.5. Reglamentación de Controles Criptográficos

En la Agencia Nacional Digital se deben utilizar los controles criptográficos o de cifrado de la información, cumpliendo con los acuerdos, legislación y reglamentación vigente; y a las buenas prácticas adoptadas.

En la Agencia Nacional Digital para la adquisición de herramientas criptográficas se debe validar la regulación sobre la importación del hardware o software en caso de ser compradas en otro país. Dicha

evaluación debe ser realizada por el Comité de Seguridad de la Información y Privacidad de los Datos Personales.

En la Agencia Nacional Digital se debe restringir el uso de cifrado de la información conforme a la clasificación de la misma, y ser evaluado por los Líderes de Proceso con el Oficial de Protección de Datos Personales, el Oficial de Seguridad de la Información y el Proceso de Gestión de Tecnologías de la Información.

La Agencia Nacional Digital 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.

18.2. Revisiones de Seguridad de la Información y Privacidad de los Datos Personales

En la Agencia Nacional Digital se debe proteger la información validando que se implementen las políticas y procedimientos establecidos.

18.2.1. Revisión Independiente de la Seguridad de la Información y Privacidad de los Datos Personales

La gestión de la seguridad de la información y privacidad de los datos personales en la Agencia Nacional Digital se debe revisar por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales de manera independiente y periódica mínimo una vez por trimestre, por cambios en el desarrollo de la misma, o cuando sea requerida.

En cada Proceso se deben monitorear el cumplimiento de las políticas de seguridad de la información y privacidad de los datos personales en su respectiva área y proceso; y notificar de manera oportuna cualquier incumplimiento al responsable de la falta, dando a conocer las causas y evidencias de la misma. Así mismo, debe reportar la falta al Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales a través del *formato de notificación y gestión de incidentes de seguridad de la información y privacidad de los datos personales*, con el fin de tomar las medidas correctivas necesarias para mejora del proceso.

La Dirección en conjunto con el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben revisar cuando se requiera el cumplimiento actual de la seguridad de la información y privacidad de los datos personales, con el fin de considerar o establecer oportunidades de mejora y realizar cambios en las políticas o controles de la seguridad que conlleven a mantener el cumplimiento de misión y visión de la Agencia Nacional Digital.

Control Interno debe realizar revisiones periódicas mínimo una vez al año sobre el sistema de gestión de seguridad de la información y privacidad de los datos personales, el cumplimiento de sus políticas y de los controles establecidos en la Agencia Nacional Digital.

Las revisiones del cumplimiento de las políticas de seguridad de la y privacidad de los datos personales deben ser documentadas y almacenadas de manera segura y protegida del personal no autorizado.

18.2.2. Cumplimiento con las Políticas y Normas de Seguridad

En la Agencia Nacional Digital, la Dirección, Subdirecciones y Líderes de Proceso, deben monitorear el cumplimiento del procesamiento de información de su área frente a las políticas, procedimientos y demás requisitos de seguridad de la información y privacidad de los datos personales establecidos. Para esto, se puede apoyar en los reportes emitidos por herramientas tecnológicas sobre el cumplimiento de las políticas en los sistemas de información de su proceso. Así mismo, debe tener presente la revisión del cumplimiento de las políticas a nivel de recurso humano.

En caso de encontrarse una no conformidad de cumplimiento de las políticas en la revisión se debe:

- Informar al Oficial de Seguridad de la Información y al Oficial de Protección de Datos Personales la no conformidad, el cual debe ser registrada en el *formato de notificación y gestión de incidentes de seguridad de la información y privacidad de los datos personales.*
- Identificar las causas o fuentes del incumplimiento.
- Identificar y definir las acciones o medidas correctivas para cumplir las políticas.
- Implementar los controles o medidas correctivas establecidas.
- Verificar la eficacia de los controles implementados realizando una nueva revisión sobre la no conformidad encontrada.

Los resultados de las revisiones realizadas sobre el cumplimiento de las políticas en los procesos deben ser registrados en un *formato de notificación y gestión de incidentes de seguridad de la información y privacidad de los datos personales*, el cual permitan llevar una trazabilidad de dichas revisiones. Así mismo, dichos registros deben ser almacenados y custodiados de manera segura, protegidos del acceso no autorizado de acuerdo con los lineamientos de protección de los registros dados en este documento.

Los Líderes de Proceso puede realizar revisiones de seguridad de la información y privacidad de los datos personales de manera independiente sobre su área y proceso a manera de autoevalulación, con fines de mejora en los controles implementados. Dichos resultados, debe reportarlos a Control Interno, al Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.

18.2.3. Revisión del Cumplimiento Técnico

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con sus equipos de trabajo deben revisar periódicamente cada tres meses o cuando sea requerido los sistemas de información de la Agencia Nacional Digital frente al cumplimiento de las políticas, procedimientos, y requisitos de seguridad de la información y privacidad de los datos personales establecidos.

En la Agencia Nacional Digital se debe revisar el cumplimiento de las *políticas de seguridad de la información y privacidad de los datos personales* aplicadas a los sistemas de información, aplicando procesos manuales y/o herramientas tecnológicas que puedan apoyar un monitoreo de los controles aplicados. Este monitoreo debe ser realizado por el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales con el apoyo del Proceso de Gestión de Tecnologías de la Información.

En la Agencia Nacional Digital se deben realizar pruebas de seguridad a través de análisis de vulnerabilidades o pruebas de intrusión de acuerdo con el alcance que se establezca a nivel interno y/o con los Terceros con las cuales se contrata o acuerda un servicio, el cual determinen el cumplimiento técnico de los controles de seguridad de la información y privacidad de los datos personales aplicados en los sistemas de información e infraestructura tecnológica. Dichas pruebas de seguridad deben ser realizadas mínimo dos (2) veces al año a la infraestructura tecnológica crítica o cuando sea requerido para el desarrollo y puesta en producción de herramientas tecnológicas desarrolladas, adquiridas o contratadas por la Agencia Nacional Digital.

En la Agencia Nacional Digital las pruebas de seguridad deben ser realizadas por personal competente y especializado a nivel interno o con empresas especialistas contratadas, cuando sea requerido.

El Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales deben determinar los planes de tratamiento para la mitigación de las vulnerabilidades técnicas sobre la infraestructura tecnológica, los sistemas de información y las aplicaciones evaluadas, quien a su vez, con el apoyo del Proceso de Gestión de Tecnologías de la Información deben aplicar los controles pertinentes para mejorar la seguridad de la información y privacidad de los datos personales, según se encuentre al alcance en términos de recursos propios de la Agencia. En caso de no ser posible aplicarlos internamente, se debe llevar el caso al Comité de Seguridad de la Información y Privacidad de los Datos Personales, quien a su vez autoriza o no, la transferencia de la aplicación de los controles a entidades especializadas con los respectivos requisitos de seguridad con el Tercero.

19. CUMPLIMIENTO

El incumplimiento de esta Política puede dar lugar a faltas disciplinarias y sanciones internas, así como a consecuencias legales, de acuerdo con la normatividad aplicable y los procedimientos establecidos por la Agencia Nacional Digital.

20. REVISIONES DE USO Y APROPIACIÓN

El delegado del Comité de Gestión y Desempeño Institucional o quien haga sus veces, debe verificar el cumplimiento de la Política, apoyado de Control Interno y los Líderes de Proceso mediante revisiones de la implementación de los procesos y procedimientos, dentro del marco del Modelo de Planeación y Gestión Institucional – MIPG.

21. VIGENCIA DE LA POLÍTICA

La política se debe revisar y actualizar una vez al año, cuando se presenten cambios organizacionales, culturales, del entorno, operativos o normativos que afecten a la Entidad. Así mismo, debe ser revisada cuando ocurran cambios de alcance que obliguen a su fortalecimiento, o de acuerdo con los resultados de las actividades de seguimiento y control definidos.

22. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	3/10/2018	Emisión del documento
2	14/05/2020	Actualización y articulación con la Norma ISO 27001 v. 2013

LESLY CRISTINA GOMEZ JARAMILLO
Firmado digitalmente por LESLY CRISTINA GOMEZ JARAMILLO
Fecha: 2020.05.28 20:55:08 -05'00'

LESLY CRISTINA GÓMEZ JARAMILLO
Directora

Revisó y aprobó: Comité Institucional de Gestión y Desempeño, sesión 14 de mayo de 2020.
Elaboró: Equipo Seguridad de la Información, Dirección AND