CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES 3
4. DOCUMENTOS DE REFERENCIA 11
5. POLÍTICAS 11
5.1.ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES 11
5.1.1. ORGANIZACIÓN INTERNA 11
5.1.2. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE PROYECTOS 12
5.2. DISPOSITIVOS MÓVILES Y TRABAJO VIRTUAL 12
5.2.1. USO DE DISPOSITIVOS MÓVILES 12
5.2.2. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA EL TRABAJO VIRTUAL 13
5.3. SEGURIDAD DE LOS RECURSOS HUMANOS 16
5.4. GESTIÓN DE ACTIVOS 17
5.4.1. MANEJO DE ACTIVOS DE INFORMACIÓN 19
5.4.2. MANEJO Y GESTIÓN DE MEDIOS REMOVIBLES 19
5.4.3. DISPOSICIÓN DE LOS MEDIOS 20
5.4.4. TRANSFERENCIA DE MEDIOS 21
5.5. ETIQUETADO DE LA INFORMACIÓN 21
5.6. CONTROL DE ACCESO 21
5.6.1. RESPONSABILIDADES DE LOS USUARIOS EN CONTROL DE ACCESO 23
5.6.2. ACCESO Y SERVICIOS A REDES 24
5.6.3 CLAVES DE ACCESO 25
5.7. CONTROL DE INGRESO SEGURO 26
5.8. USO DE PROGRAMAS UTILITARIOS 27
5.9. CONTROL DE ACCESO A CÓDIGOS FUENTE DEL SOFTWARE 27
5.10. CRIPTOGRAFÍA Y GESTIÓN DE LLAVES 27
5.11. SEGURIDAD FÍSICA Y DEL ENTORNO 30
5.11.1.CONTROLES DE ACCESO FÍSICO 30
5.12. EQUIPOS 31
5.13. ESCRITORIO LIMPIO Y PANTALLA DESPEJADA 32
5.14. SEGURIDAD DE LAS OPERACIONES 33
5.14.1.GESTIÓN DE CAMBIOS 33
5.14.2.GESTIÓN DE LA CAPACIDAD 33
5.14.3.SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN 34
5.14.4.CONTROLES CONTRA CÓDIGOS MALICIOSOS 34

5.15. COPIAS DE RESPALDO DE INFORMACIÓN 35
5.16. REGISTRO Y SEGUIMIENTO Y PROTECCIÓN DE EVENTOS 37
5.17. CONTROL DE SOFTWARE OPERACIONAL Y RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE 37
5.18. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS 38
5.19. SEGURIDAD DE LAS COMUNICACIONES 39
5.19.1.GESTIÓN DE LA SEGURIDAD DE LAS REDES 39
5.19.2.TRANSFERENCIA DE INFORMACIÓN Y ACUERDOS DE CONFIDENCIALIDAD 41
5.20. CIBERSEGURIDAD 42
5.21. USO DE SERVICIOS DE CORREO ELECTRÓNICO 43
5.22. USO DE SERVICIO DE ACCESO A INTERNET 43
5.23. ADQUISICIÓN, DESARROLLO SEGURO Y MANTENIMIENTO DE SISTEMAS 44
5.23.1.CONTROL DE CAMBIOS EN SISTEMAS DE INFORMACIÓN 45
5.23.2.PRINCIPIOS EN LA CONSTRUCCIÓN DE SISTEMAS SEGUROS 45
5.23.3.PROTECCIÓN DE LOS DATOS DE PRUEBA 46
5.24. RELACIONES CON LOS PROVEEDORES 46
5.24.1.SEGUIMIENTO Y REVISIÓN DE SERVICIOS DE LOS PROVEEDORES 47
5.24.2.GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES 47
5.25. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES 47
5.26. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO 48
5.27. CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN 50
5.28. DERECHOS DE AUTOR Y PROPIEDAD INTELECTUAL 50
5.29. PROTECCIÓN DE REGISTROS 51
5.30. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES 52
6. CUMPLIMIENTO 52
7. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES 52
8. VIGENCIA DE LA POLÍTICA 53
9. CONTROL DE CAMBIOS 53

1. OBJETIVO

Establecer lineamientos para preservar la confidencialidad, integridad y disponibilidad de la información en la Agencia Nacional Digital, a través de la implementación del Sistema de Gestión de Seguridad de la Información y Privacidad de los Datos Personales (SGSI–PDP), conforme al cumplimiento de los requisitos legales, estratégicos, operativos, tecnológicos y tácticos.

2. ALCANCE

Aplica a todos los procesos, áreas y/o dependencias de la Agencia Nacional Digital. Aplica de igual manera a todos los activos de información que hacen parte de la infraestructura tecnológica y de seguridad 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 presentes políticas.

3. DEFINICIONES

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 resultar en daño a un sistema u organización. [ISO/IEC 27000:2018].

e) Amenaza informática: 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 de comprender la naturaleza del riesgo y determinar el nivel de riesgo. [ISO/IEC 27000:2018]. 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 estas, 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 corporativos y 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: Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].

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

s) 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.

t) Control: Es una medida que modifica el riesgo. [ISO/IEC 27000:2018]. 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.

u) 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 esta y pueda estar disponible.

v) 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.

w) 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).

x) 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).

y) Dato personal: hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

z) 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.

aa) Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

bb) 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.

cc) Dato semiprivado: Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad general, como es el caso de los datos financieros y crediticios de la actividad comercial o de servicios.

dd) Disponibilidad: Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018].

ee) 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.

ff) 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].

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

gg) Responsable del Tratamiento: Es toda persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre las bases de datos y/o el Tratamiento de los datos. Para efectos de esta Política, el responsable del Tratamiento es la Agencia Nacional Digital.

hh) Evento de seguridad de la información: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000:2018]. 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.

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

jj) 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.

kk) Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. [ISO/IEC 27000:2018].

ll) 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.

mm) Impacto: Cambio adverso en el nivel de los objetivos del negocio logrado. [ISO/IEC 27000:2018].

nn) Incidente de seguridad de la información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000:2018].

oo) 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 estrategia de continuidad del negocio.

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

qq) Incidente de 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.

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

ss) Integridad: Propiedad de exactitud y completitud. [ISO/IEC 27000:2018].

tt) 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.

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

vv) 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].

ww) Norma: Principio que se dispone de carácter general, donde se establecen las obligaciones, restricciones y orientaciones para el acceso y uso de los activos de información.

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

yy) 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.

zz) 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.

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

bbb) Política: Intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000:2018].

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

ddd) Probabilidad: Frecuencia o Factibilidad de ocurrencia del Riesgo. [ISO/IEC 27000:2018].

eee) Procedimiento: Documento que define los pasos a seguir y que serán implementados en una situación dada.

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

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

hhh) 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.

iii) Riesgo: Efecto en la incertidumbre de los objetivos [ISO/IEC 27000:2018]..

jjj) 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.

kkk) 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)).

lll) 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).

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

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

ooo)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, implantación, 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).

ppp)Titular de la información: Persona natural y jurídica cuyos datos personales sean objeto de tratamiento.

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

rrr) Trabajo virtual: actividad laboral o contractual que se desarrolla fuera de las instalaciones de la entidad, a través de herramientas tecnológicas que permiten el trabajo seguro de acuerdo con el cumplimiento de las políticas de seguridad y privacidad de la información.

sss) 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.

ttt) Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2018].

uuu) 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.

4. DOCUMENTOS DE REFERENCIA

- Normograma de la Entidad (publicado en la página web en el enlace de transparencia y acceso a la información en el numeral 4. Normatividad)

5. POLÍTICAS

5.1. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES

5.1.1. Organización interna

La Agencia Nacional Digital establece una estructura en torno al manejo de la seguridad de la información y privacidad de los datos personales. Así es como ha conformado el proceso de Seguridad y Privacidad de la Información a nivel estratégico como parte de la Alta Dirección, dando direccionamiento y gestión como eje transversal en toda la Entidad y operaciones.

Se debe establecer y mantener contacto con las autoridades pertinentes en materia de Seguridad de la Información, con el fin de dar cumplimiento a la legislación y normativas internas y externas vigentes.

Se debe contar con la lista de contactos con las autoridades, empresas de servicios públicos (energía, agua, seguridad, comunicaciones), servicios de emergencia y departamentos de bomberos.

Se debe informar a las autoridades competentes cuando sea el caso sobre los ataques o delitos cibernéticos que llegasen a presentarse, con el fin de que se adelanten las acciones pertinentes.

Mantener contacto con grupos especialistas en materia de seguridad de la información y ciberseguridad, así mismo establecer alianzas estratégicas con organizaciones, foros y/o eventos que permitan adquirir, fortalecer y fomentar el conocimiento de las mejores prácticas de seguridad, 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, entre otros temas de interés.

Todos los roles que desempeñen funciones laborales o actividades contractuales relacionadas con Seguridad de la Información deben hacer parte del proceso de Seguridad y Privacidad de la Información.

5.1.2. Seguridad de la información y privacidad de los datos personales en la gestión de proyectos

La Agencia Nacional Digital debe contar con información documentada de seguridad en la Gestión de Proyectos, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

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

Los requisitos de seguridad de la información y privacidad de los datos personales en todos proyectos deben ser definidos por el proceso de Seguridad y Privacidad de la Información, los cuales deben ser aceptados e implementados por los Gerentes y responsables de los Proyectos, quien a su vez se encargarán de velar por su cumplimiento en cada proyecto que se lleve a cabo realizando revisiones periódicas a través de los mecanismos establecidos en la Agencia para la Gestión de Proyectos.

Se deben contemplar los Riesgos de Seguridad y privacidad asociados a la Gestión de Proyectos.

Cualquier incumplimiento de los requisitos de seguridad de la información y privacidad de los datos personales establecidos para los proyectos deben ser informados oportunamente por el supervisor del contrato, Gerente o responsable del Proyecto a las partes interesadas incluyendo a Seguridad de la Información para tomar las acciones necesarias.

Los supervisores de contratos, Gerentes o responsables de los proyectos deben reportar los incidentes, eventos o riesgos de seguridad, con el fin de dar aplicar el *procedimiento de notificación y gestión de incidentes de seguridad de la información* y la *metodología de Gestión de riesgos.*

5.2. DISPOSITIVOS MÓVILES Y TRABAJO VIRTUAL

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

5.2.1. 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:

- Los procesos de Seguridad y Privacidad de la Información y TI deben evaluar los requisitos mínimos de seguridad y privacidad en los dispositivos móviles personales que porten sus empleados de planta y/o contratistas para el desarrollo de sus actividades laborales o contractuales.

- El uso de dispositivos móviles institucionales es de uso exclusivo para el desarrollo de actividades laborales o contractuales según sea el caso.
- Los Empleados de Planta y Contratistas que utilizan dispositivos móviles personales son responsables de acatar las medidas de seguridad de la información y privacidad de los datos personales e informar oportunamente a su jefe inmediato o Supervisor de Contrato cualquier incidente o riesgo en el cual se vea afectada la información o los datos de la Agencia Nacional Digital.
- No descargar información de la Agencia Nacional Digital en otros dispositivos no autorizados o en repositorios personales sin previa autorización del proceso de seguridad y privacidad de la información.
- Todos los dispositivos en los que se procese, almacene o transmita información de la Agencia deben aplicar las políticas de seguridad y privacidad de la información.
- Todos los dispositivos móviles autorizados o adquiridos en la Agencia deber ser registrado en el inventario de activos de información.
- Todo dispositivo móvil debe estar debidamente licenciado ya sea con software comercial u open source.
- Se debe hacer buen uso de los dispositivos móviles otorgados por la Agencia.
- La subdirección administrativa y financiera es la responsable de controlar a nivel tecnológico el uso de dispositivos móviles.
- El uso de los dispositivos móviles personales debe realizarse creando una sesión independiente para el desarrollo de las actividades laborales y/o contractuales.
- Se debe almacenar la información en los repositorios autorizados por la Entidad.
- Evitar almacenar información en los dispositivos móviles personales.
- El soporte y mantenimiento del software y hardware para los dispositivos personales previamente aprobados por la Entidad, será responsabilidad del usuario.

5.2.2. Seguridad y privacidad de la información para el trabajo virtual

La Agencia Nacional Digital reconoce el trabajo virtual como una opción para el desarrollo de las actividades laborales o contractuales de sus colaboradores en razón con el cumplimiento de su misión, de acuerdo con el tipo de contrato suscrito y de la modalidad que se establezca para tal fin, conforme a la legislación colombiana, sea mediante, teletrabajo, trabajo remoto o trabajo en casa independientemente del lugar de ubicación para el desarrollo de las actividades laborales o contractuales. En cumplimiento de lo anterior, y con el ánimo de proteger la información y los datos se establecen los lineamientos de seguridad y privacidad de la información de la siguiente manera:

- **Ubicación del colaborador y acceso a los activos de información**

Es responsabilidad de los colaboradores (empleados de planta, contratistas y terceros), aplicar los lineamientos de seguridad y privacidad de la información para desarrollar sus actividades laborales o contractuales fuera de las instalaciones de la AND.

Se debe realizar la identificación y análisis de riesgos de seguridad y privacidad de la información en conjunto con los procesos de gestión de talento humano y jurídica, a través de los instrumentos establecidos para tal fin al interior de la AND, con el fin de evaluar el nivel de protección de la información y los datos.

Se debe realizar una conexión segura a través de VPN (Virtual Protocol Network), entre otras establecidas por la Agencia.

Está prohibido el uso de redes públicas (aeropuertos, café internet, entre otros), para el ejercicio o desarrollo de las actividades laborales o contractuales que realicen los colaboradores (empleados de planta, contratistas o terceros).

Para asistir a las actividades virtuales de la entidad a través del correo electrónico corporativo cumpliendo los lineamientos de seguridad y privacidad de la información. Así mismo, cambiar la contraseña del WiFi mínimo 1 vez cada 3 meses.

Se debe contar con una red WPA2 con clave que cumpla con los lineamientos de la política de claves de acceso establecidos en el numeral 10.3 del presente documento.

Se debe crear una sesión independiente de trabajo si el equipo es personal, si es asignado por la Agencia sólo debe hacerse uso para fines laborales y contractuales.

Se debe realizar el almacenamiento de la información en los repositorios dispuestos por la Agencia de acuerdo con lo establecido por el proceso de gestión documental.

Dar cumplimiento a las políticas de control de acceso establecidas en el numeral 10 del presente documento.

Se debe contar con licencias del software en los dispositivos desde los cuales se realizan las actividades laborales o contractuales por los colaboradores (empleados de planta, contratistas y terceros), de acuerdo con la política de gestión de activos (numeral 8) y política de derechos de autor y propiedad intelectual (numeral 32) del presente documento.

- **Obligaciones para salvaguardar y custodiar la seguridad y privacidad de la información en el trabajo virtual**

Los colaboradores (empleados de planta, contratistas o terceros), son responsables de la seguridad y privacidad de la información y los datos que manejan en sus activos, de acuerdo con los lineamientos, controles y políticas establecidas por la entidad.

Bloquear o apagar el equipo cuando no esté en uso, con el fin de proteger la información y los datos, de accesos no autorizados.

Realizar cambio de contraseñas de acuerdo con la política de control de acceso establecida en el numeral 10.3 del presente documento.

El incumplimiento de las políticas de seguridad y privacidad de la información por parte de los empleados de planta estará sujeto a las medidas disciplinarias de acuerdo con el reglamento interno de trabajo y el procedimiento disciplinario establecido por la AND.

El incumplimiento de las políticas de seguridad y privacidad de la información por parte de los contratistas, proveedores y terceros, en concordancia con el clausulado general del contrato de prestación de servicios, podrá ser sujeto de declaratoria de posible incumplimiento, de conformidad con el procedimiento establecido por la Agencia.

Todos los colaboradores (empleados de planta, contratistas y terceros), son responsables 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 contractuales y la que se genere de la misma.

- **Del soporte y mantenimiento de los equipos en el trabajo virtual**

El proceso de gestión de tecnologías de la información y el proceso de gestión administrativa son responsables de gestionar el soporte y mantenimiento del hardware y software de dispositivos institucionales para el desarrollo del trabajo virtual, de acuerdo con la política de adquisición, desarrollo y mantenimiento de sistemas establecida en el numeral 27 del presente documento.

Los dispositivos personales utilizados por los colaboradores (empleados de planta, contratistas o terceros) para el desarrollo de las actividades laborales o contractuales, no son sujetos de soporte y mantenimiento por parte de la Agencia.

El proceso de gestión administrativa debe contar con pólizas de seguro para los dispositivos de la entidad, incluyendo los asignados al trabajo virtual.

5.3. SEGURIDAD DE LOS RECURSOS HUMANOS

La Agencia Nacional Digital debe implementar los controles necesarios para contratar e identificar de manera idónea el personal que va a ejecutar actividades laborales o contractuales en la Entidad.

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

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.

Se debe notificar de los cambios administrativos y contractuales al proceso de Seguridad y Privacidad de la Información semanalmente o por demanda de acuerdo con los cambios que se presenten.

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 de no divulgación.

En todos los contratos laborales, contractuales y acta de posesión se debe incluir una cláusula de confidencialidad y no divulgación.

Se deben establecer los términos y condiciones del empleo, las responsabilidades propias de sus funciones en seguridad de la información y privacidad de los datos personales para Empleados de Planta, Contratistas y terceros cuando sea el caso.

Todos los Empleados de Planta, Contratistas y Terceros deben dar cumplimiento a las políticas y lineamientos establecidos en seguridad y privacidad de la información.

Se debe capacitar y sensibilizar en seguridad de la información y protección de datos personales al personal de plana, contratistas y terceros cuando sea el caso a través de inducciones o reinducciones en la Entidad.

Se deben incluir los temas de seguridad de la información y protección de datos personales en el plan de capacitación institucional anual de la Entidad.

Se debe establecer y divulgar un proceso formal de control disciplinario, el cual debe incluir los posibles incumplimientos o violaciones a la seguridad de la información y privacidad de los datos personales.

Se debe establecer los controles necesarios para la protección de la información de la Entidad, frente a la terminación o cambio de roles o funciones en contratos de Empleados de Planta, Contratistas y Terceros.

Se debe firmar el acuerdo de confidencialidad y privacidad de la información por parte de todos los colaboradores.

El proceso de Gestión de Talento Humano debe realizar el envío de las novedades administrativas mensualmente o por demanda cuando sea el caso para realizar una adecuada gestión de accesos.

5.4. GESTIÓN DE ACTIVOS

La Agencia Nacional Digital debe gestionar los activos de información conforme a las políticas y procedimientos establecidos, realizando la identificación, valoración, clasificación y mejora continua de los mismos.

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

Los líderes de proceso o quien hagan sus veces, son responsables de identificar y registrar en la matriz definida los activos de información de su proceso.

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

Cada activo de información tiene designado un propietario y responsable en el inventario de activos, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

Se debe establecer el proceso formal de disposición de medios fuera de las instalaciones, con el fin de llevar la trazabilidad de los activos de información que son retirados de la Entidad.

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

Todos los Empleados de Planta, Contratistas y terceros cuando sea el caso deben realizar copia de seguridad de toda la información clasificada como Publica Clasificada y Pública Reservada que se encuentra almacenada o que se genere en el equipo que tiene asignado.

Todos los equipos de cómputo de la Agencia deben tener instalado el software antimalware otorgado por la Entidad y debe estar configurado de acuerdo con las políticas establecidas.

Todos los Empleados de Planta, Contratistas y terceros cuando sea el caso 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.

Todos los Empleados de Planta, Contratistas y terceros cuando sea el caso deben reportar, cualquier evento o incidente que pueda afectar la Confidencialidad, integridad y disponibilidad de la información.

Todos los Empleados de Planta, Contratistas y terceros cuando sea el caso deben aplicar la metodología de gestión de riesgos institucional, para identificar y tratar los riesgos de seguridad de la información y privacidad de los datos personales que puedan afectar a los activos de información a su cargo.

Todas las modificaciones o actualizaciones de los activos de información tecnológicos deben cumplir con el *Procedimiento de Gestión de Cambios* establecido por la Entidad.

Todos los Empleados de Planta, Contratistas y terceros cuando sea el caso deben dar cumplimiento a las políticas y controles de seguridad de la Información establecidos para tratar los riesgos que pueda afectan la seguridad de la información y privacidad de los datos personales.

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

1. Incumplimiento de las políticas de seguridad y privacidad de la información y datos personales.
2. Mal uso o abuso de los activos de información que se encuentran bajo su custodia o propiedad.
3. Modificación de la información sin previa autorización.
4. Divulgación no autorizada de información.
5. Impedir el acceso a la información sin una justificación valida.
6. Modificación o eliminación de los controles de seguridad.
7. 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.
8. 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.
9. Hacer uso de software ilegal o no licenciado.

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 los procesos establecidos por la Agencia.

En la Agencia Nacional Digital establecerá 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.

5.4.1. 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 confidencialidad, integridad y disponibilidad de las copias de respaldo de información y datos personales, de acuerdo con los procedimientos y plan de copias de respaldo de información establecidos en la Entidad.

5.4.2. Manejo y gestión de medios removibles

Se debe controlar la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de acuerdo con los lineamientos establecidos por la Entidad.

Los medios removibles como (USB, Discos Externos, cámaras fotográficas, cámaras de video, celulares, portátiles, entre otros), que hacen parte de la operación de la Agencia serán 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 con los lineamientos establecidos para tal fin.

Para el retiro de cualquier medio de almacenamiento, se debe realizar de acuerdo con los lineamientos establecidos, el cual debe permitir llevar la trazabilidad de quien retira, quien autoriza, en qué fecha, tipo de dispositivo, etc.

Se debe tener un propietario asignado para cada activo, quien tendrá bajo su responsabilidad asegurar la confidencialidad, integridad y disponibilidad del este. Así mismo debe almacenarlo de manera segura.

Los dispositivos que se encuentren fuera de las instalaciones deben tener almacenada la información de manera segura, en lo posible cifrada, controlando el acceso de personal no autorizado.

Los propietarios de los activos deben informar a las partes interesadas (Subdirección Administrativa y Financiera, Tecnologías de la Información, Seguridad de la Información, entre otras si es el caso) el deterioro o riesgos que representa la información almacenada en los medios, con el fin de tomar las acciones necesarias para la protección de la información y datos personales.

Los propietarios de los medios deben realizar copias de respaldo de información, de acuerdo con los lineamientos establecidos.

Los medios de almacenamiento temporal (USB, DVD/CD, Discos Externos), no deben utilizarse como copias de información.

El uso de medios de almacenamiento de la información será restringido solo para personal autorizado.

La transferencia de medios debe realizarse de acuerdo con los procesos formales establecidos por la Agencia.

5.4.3. Disposición de los Medios

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 estos, por motivos de retiro, obsolescencia, cambio u otros.

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 y de seguridad debe realizarse previa autorización por las partes interesadas y por el proceso de Gestión de Tecnologías de la Información.

5.4.4. Transferencia de medios

Se debe asegurar que la información que se transporta a través de los medios físicos está protegida de acceso por personal no autorizado y libre de cualquier alteración.

Para el transporte y disposición de los medios, se debe llevar la trazabilidad a través de los lineamientos establecidos por la Agencia.

Se debe contar si es el caso con acuerdo de confidencialidad y transferencia de medios e información.

5.5. ETIQUETADO DE LA INFORMACIÓN

Todos los Empleados de Planta, Contratistas y Terceros cuando sea el caso, deben mantener organizado el archivo de gestión físico y digital, siguiendo los lineamientos establecidos por la Entidad y de acuerdo con la clasificación de la información establecida.

La plataforma tecnológica dispuesta para almacenar y conservar la información debe asegurar los principios fundamentales de la seguridad como son la confidencialidad, integridad 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.

5.6. CONTROL DE ACCESO

La Agencia Nacional Digital limita el acceso a los activos de información como sistemas de información, aplicaciones, instalaciones, correo electrónico, redes, etc., con el fin de asegurar la confidencialidad, integridad y disponibilidad de esta.

La Entidad debe establecer lineamientos y procedimientos formales de control de acceso, con el fin de proteger la información y llevar la trazabilidad en cuanto uso por parte del personal autorizado.

Se debe elaborar y hacer mantenimiento a la matriz de roles y permisos de acceso a los activos de información, por los procesos de Gestión de Tecnologías de la Información, Gestión de Talento Humano, Seguridad y Privacidad de la Información.

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 Proceso o quien haga sus veces.

Los privilegios deben limitarse al mínimo de permisos para cumplir con sus responsabilidades según lo determine su rol.

Todo acceso físico o lógico, asignado a los Empleados de Planta, Contratistas y Terceros debe ser desactivado o modificado una vez finalice el vínculo laboral o contractual con la Entidad

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 personal e intransferible.

Se debe realizar mantenimiento y revisiones periódicas de usuario, roles y permisos que tienen acceso a los activos de información de la Entidad.

Realizar revisiones mínimo una vez cada 6 meses de los usuarios por parte del proceso de Seguridad y privacidad de la Información.

Todos los usuarios que no se encuentren en uso en un periodo igual o superior a 45 días, se deben inactivar durante 15 días, si posterior a este tiempo no se realiza ninguna solicitud al respecto, se debe hacer copia de respaldo de la cuenta y eliminarlo si es el caso.
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.

Los usuarios y claves de acceso a los activos de información autorizados son personales e intransferibles y no deben ser compartidos, en caso de que por fuerza mayor lo realicen, se debe notificar a Seguridad de la Información para su documentación y una vez se encuentre en la red de la Agencia debe realizar el cambio.

Los Empleados de Planta, Contratistas y Terceros deben establecer una contraseña segura, teniendo en cuenta la política de Gestión de Contraseñas.

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

El proceso de Gestión de Talento Humano debe enviar cada mes a Seguridad de la Información y las partes interesadas, las novedades administrativas (retiros, traslados, ingresos, incapacidades, vacaciones, etc.), con el finde realizar la cancelación definitiva o temporal de los accesos.

Se debe contar con el acceso de lectura al archivo o sistema de información de contratación, con el fin de poder validar las terminaciones, sesiones, suspensiones, etc de los contratos de persona natural y jurídica cuando sea el caso.

Se debe contar con doble factor de autenticación para los usuarios administradores o privilegiados, con el fin de fortalecer el control de accesos a estos activos de información.

Se debe realizar cambio de claves de acceso cuando se realice cambio de proveedores que administran las herramientas o cuando un colaborador termine su vínculo laboral o contractual con la Agencia.

Toda asignación de información de autenticación secreta (usuarios y contraseñas), se realizará a través de medios seguros de comunicación y de acuerdo con los lineamientos establecidos por la Agencia.

La información de accesos privilegiados debe entregarse y almacenarse de manera seguro, de acuerdo con la política de cifrado de la información.

5.6.1. Responsabilidades de los usuarios en control de acceso

Todos los Empleados de Planta, Contratistas o Terceros cuando sea el caso son responsables de:

- Hacer buen uso de los usuarios y claves de acceso.
- Almacenar las credenciales de acceso de manera segura.
- Mantener la confidencialidad de la información de registro en los activos 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 activos de información de la Agencia.
- Cambiar la clave de acceso mínimo una vez cada 30 días.
- Crear contraseñas fuertes, de calidad, sencillas de recordar y difíciles de adivinar.
- Cambiar al primer inicio de sesión las contraseñas genéricas otorgadas para el acceso a los activos de información solicitados.
- No se debe usar la misma contraseña para el ingreso a varios sistemas de información.
- No usar las contraseñas de uso personal para uso institucional o viceversa.

- doble factor de autenticación para los usuarios administradores o privilegiados, con el fin de fortalecer el control de accesos a estos activos de información.
- Los administradores de activos de información deben realizar cambio de claves de acceso cuando haya cambio de proveedores o cuando un colaborador termine su vínculo laboral o contractual con la Agencia.
- Los administradores deben cambiar las claves de acceso a los activos de información que administran mínimo una vez cada 4 meses.

5.6.2. Acceso y Servicios a Redes

Se deben definir los roles y perfiles de acceso a la red y parametrizarlos en las herramientas que corresponda.

Todos los accesos requeridos, se deben tramitar a a través del procedimiento formal de control de accesos establecidos en la Agencia.

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

Se debe realizar conexión remota a la red de área local de la Agencia a través de una conexión seguridad como VPN (Virtual Private network o Red Privada Virtual).

Proteger las redes contra accesos no autorizados implementando soluciones que permitan monitoreo y generación de alertas.

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

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.

Se deben crear segmentos de red independientes para los servidores, parte administrativa y visitantes.

5.6.3 Claves de Acceso

La Agencia Nacional Digital establece el procedimiento de control de acceso, con el fin de llevar la trazabilidad de la gestión de usuarios y claves de accesos.

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

Las contraseñas de acceso a los activos de información deben tener una complejidad como la que se muestra a continuación, si la tecnología o el activo de información no lo permite, se debe establecer planes de acción alternativos para la protección de la información:

- Longitud mayor o igual a 9 caracteres
- Contener Mayúsculas y minúsculas
- Números
- Por lo menos un carácter especial
- Realizar 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

En caso de requerir la creación de un usuario genérico se debe establecer un responsable de su administración.

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 claves 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
- Mecanismos de autenticación habilitado para el ingreso a la red
- Revisión y aval por parte de los procesos de Gestión de Tecnologías de la Información y Seguridad y Privacidad de la Información.

5.7. CONTROL DE INGRESO SEGURO

El acceso a activos de información críticos de la Agencia Nacional Digital se realizará de acuerdo con los lineamientos establecidos en el procedimiento de ingreso seguro.

Los sistemas de autenticación deben mantener un registro o logs de auditoría que permitan llevar la trazabilidad de los ingresos y acciones realizadas.

Al acceso a los activos de información críticos deben incluirse siempre y cuando la tecnología lo permita en el correlacionador de eventos – SIEM adquirido por la Entidad.

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.

No se deben visualizar los identificadores de ingreso al sistema o aplicación (usuario y contraseña.

Se deben parametrizar mensajes que permitan al usuario orientarse para el acceso seguro a los activos de información.

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.

5.8. 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, de acuerdo con los lineamientos establecidos para tal fin.

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.

Todos los usuarios que requieran instalar un programa utilitario deben solicitarlo al Proceso de Seguridad y Privacidad de la Información a través del correo seguridaddigital@and.gov.co.

5.9. CONTROL DE ACCESO A CÓDIGOS FUENTE DEL SOFTWARE

Los códigos fuente de todo el software desarrollado o adquirido por terceros propiedad o uso de la Agencia Nacional Digital será restringido solo a personal autorizado.

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

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

5.10. CRIPTOGRAFÍA Y GESTIÓN DE LLAVES

La Agencia Nacional Digital protege la confidencialidad, integridad y disponibilidad de la información pública reservada o clasificada mediante controles criptográficos, de acuerdo con la normatividad y lineamientos establecidos.

La Dirección de la Agencia Nacional Digital debe gestionar y proporcionar los recursos para la implementación de herramientas criptográficas que permitan proteger la información en sus operaciones y servicios prestados.

La Dirección de la Agencia Nacional Digital debe autorizar el uso de la criptografía mediante las herramientas tecnológicas que se hayan definido y aprobado para esta labor por parte del personal autorizado.

Los Empleados, Contratistas y Terceros autorizados deben utilizar solo las herramientas tecnológicas autorizadas por la Entidad para cifrar la información y gestión de las llaves criptográficas respectivas.

Todos los Empleados, Contratistas y Terceros de la Agencia Nacional Digital deben gestionar sus llaves criptográficas de acuerdo con los lineamientos y herramientas establecidas y autorizadas.

Todos los Empleados, Contratistas y Terceros son responsables de la custodia segura de las llaves criptográficas.

Está prohibido compartir las llaves criptográficas con personal no autorizado.

Todos los Empleados de planta o Terceros deben cambiar de inmediato cualquier llave criptográfica que haya sido perdida o presente un riesgo de pérdida de su confidencialidad.

Cualquier incidente o riesgo presentado con las llaves criptográficas debe ser notificado de inmediato al Proceso de Seguridad y Privacidad de la Información de acuerdo con los procedimientos establecidos.

Está prohibido enviar llaves criptográficas en texto claro a través de correos electrónicos o cualquier medio de comunicación autorizado por la Agencia.

Está prohibido el envío de llaves criptográficas a través de medios públicos como redes sociales.

Los Empleados, Contratistas y Terceros autorizados por la Agencia Nacional Digital deben establecer contraseñas fuertes y de alta complejidad y la seguridad adecuada sobre la gestión de las llaves criptográficas, con el fin de prevenir el acceso de personal no autorizado a la información.

Toda llave criptográfica de información que ya no se requiera para la operación o que tenga un trato histórico (para consulta), debe ser enviada a custodia conforme a los lineamientos establecidos.

Toda llave criptográfica de la información que tiene un manejo temporal en su intercambio, que su medio original se encuentra en su repositorio oficial y que dispone de una copia de acuerdo con las políticas establecidas, podrá ser desechada o eliminada de acuerdo con los lineamientos de destrucción segura de la información.

Se debe cambiar las claves o contraseñas de acceso de los sistemas de gestión de llaves criptográficas de manera periódica de acuerdo con las políticas de control de acceso establecidas.

Los sistemas de gestión de llaves criptográficas deben bloquearse por intentos fallidos para su uso de acuerdo con las políticas de control de acceso establecidas.

Los sistemas de gestión de llaves criptográficas deben evitar el uso de sesiones concurrentes conforme a las políticas de control de acceso establecidas.

La adquisición de herramientas criptográficas en la Agencia Nacional Digital se debe hacer validando previamente su parte legal, especialmente, frente a la regulación vigente en Colombia sobre derechos de autor y estándares nacional e internacionalmente aceptados.

El uso del cifrado de en la Agencia Nacional Digital se debe utilizar de acuerdo con la clasificación y riesgo de la información para su intercambio, envío o almacenamiento.

En casos de orden judicial, el cual debe entregar información para investigaciones de casos judiciales, se debe hacer de manera encriptada según lo acordado con el ente judicial.

En la Agencia Nacional Digital se utilizarán 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 los responsables para tal fin.

En la Agencia Nacional Digital se debe restringir el uso de cifrado de la información conforme a la clasificación de esta, y ser evaluado por los Líderes de Proceso y Seguridad y Privacidad de la Información en el cual indicarán qué información debe requerir de este procedimiento.

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.

5.11. 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.

Se deben establecer lineamientos para prevenir el acceso físico no autorizado, contra daño, interferencia de la información, a las instalaciones y áreas de procesamiento de información como centros de cómputo, centros de gestión documental, entre otros.

Se debe contar con la debida marcación e identificación de las áreas de procesamiento de información.

Se debe llevar el registro formal del control de acceso físico a las áreas de procesamiento de información.

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. Así mismo 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 Pública Reservada, Pública Clasificada y 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.

5.11.1. Controles de acceso físico

Se debe contar con un control de acceso fuerte, que permita realizar el registro y salida de visitantes y dispositivos móviles.

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 llevar la trazabilidad de los ingresos.

Para las áreas de procesamiento contratadas con un Tercero, la Agencia Nacional Digital le exigirá 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.

Se debe contar con controles de acceso a las instalaciones u oficinas a través de sistemas biométricos, electrónicos, entre otros.

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

Se debe contar con áreas delimitadas de carga y descarga en la Entidad.

5.12. EQUIPOS

En la Agencia Nacional Digital debe establecer lineamientos de seguridad para la protección de los equipos contra pérdida, robo o cualquier afectación que pueda poner en riesgo la información o la continuidad de las operaciones.

Se establecen 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.

Contar con un programa o plan de soporte y mantenimiento a elementos de contingencia como ups, plantas eléctricas alternas, operadores de internet alternos o con redundancia, entre otros.

Se debe contar con seguridad en 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.

Se debe contar con un programa o plan de soporte y mantenimiento a los equipos que hacen parte de sus operaciones conforme a las especificaciones de los fabricantes y buenas prácticas aplicadas.

Se debe llevar un control de los activos que se retiran de las instalaciones, de acuerdo con los lineamientos establecidos para tal fin.

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 trabajo remoto y dispositivos móviles; y a los riesgos asociados sobre el uso de estos como responsabilidad asumida por los usuarios autorizados.

Se debe realizar borrado seguro de información antes de realizar un traslado, o dar de baja un equipo.

5.13. ESCRITORIO LIMPIO Y PANTALLA DESPEJADA

La Agencia Nacional Digital define 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.

Todos los equipos de la Agencia Nacional Digital deberán ser bloqueados automáticamente después de tres (3) minutos de inactividad.

El Proceso de Gestión de Tecnologías de la Información es el responsable de establecer los controles de bloqueo sobre las sesiones de los usuarios para que se inactiven en el tiempo determinado.

Todos los empleados de planta, contratistas y terceros cuando sea el caso son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren de la misma.

Al finalizar la jornada laboral o contractual se deben cerrar todas las aplicaciones y dejar los equipos apagados o en hibernación.

Todos los empleados de planta, contratistas y terceros cuando sea el caso deben conservar su escritorio físico y virtual libre de información clasificada, que pueda ser tomada, copiada o utilizada por personal no autorizado.

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.

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.

Todos los empleados de planta, contratistas y terceros cuando sea el caso deben guardar en un lugar seguro cualquier documento y/o elementos de almacenamiento externos (CD, DVD, USB) conforme los niveles de calificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

Los archivos que contengan información sensible o confidencial deberán ser almacenados en rutas que impidan el fácil acceso por terceros no autorizados, evitando, guardarlos en el área de escritorio virtual del equipo.

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

Todos los empleados de planta, contratistas y terceros cuando sea el caso 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.

5.14. SEGURIDAD DE LAS OPERACIONES

En la Agencia Nacional Digital se documenta, revisa y aprueba todos los documentos que hacen parte de sus operaciones de acuerdo con lo requerido en cada proceso y el Sistema Integrado de Gestión de Calidad.

5.14.1. Gestión de cambios

Se deben gestionar y controlar todos los cambios que se realizan en los activos de información que puedan afectar la seguridad y continuidad de las operaciones de acuerdo con el procedimiento de gestión de cambios.

Se debe llevar el control y trazabilidad de los cambios solicitados y ejecutados en los activos de información críticos de la Entidad.

5.14.2. Gestión de la capacidad

Se debe establecer un plan de capacidades, el cual debe incluir los activos críticos de la Entidad.

Gestionar los recursos necesarios para la ejecución del plan de capacidades definido en la Entidad.

La capacidad de los activos de tecnológicos será gestionada por el Proceso de Gestión de Tecnologías de la Información, asegurando la disponibilidad de las operaciones de la Agencia Nacional Digital.

5.14.3. Separación de los ambientes de desarrollo, pruebas y producción

Se debe conta con al menos los ambientes de desarrollo, pruebas y producción de manera independiente, con el fin de proteger la información que se maneja en la Agencia Nacional Digital, sin embargo, esto no limita a contar con ambientes de QA – Calidad y Preproducción.

Estos ambientes deben disponer de reglas o controles para la transferencia de software de los ambientes de desarrollo, pruebas al de producción.

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

Cada uno de los ambientes debe contar con niveles aceptables de seguridad.

5.14.4. Controles Contra Códigos Maliciosos

Se deben proteger los activos tecnológicos contra las amenazas informáticas y malware que puedan poner en riesgo la seguridad de la información, privacidad de los datos personales, y continuidad de las operaciones.

Se deben definir e implementar controles de detección, prevención y recuperación de códigos maliciosos.

Se debe realizar sensibilización a todos los empleados de planta, contratistas y terceros de la Agencia acerca de la prevención, protección y riesgos de los malware, lo cual estará bajo la responsabilidad del Proceso de Seguridad y Privacidad de la Información.

Las partes interesadas deben analizar, evaluar y definir las herramientas de seguridad y privacidad que se deben implementar y configurar en la Agencia Nacional Digital para protección de la información y datos personales.

El proceso de Tecnología será responsable de implementar y controlar las herramientas de seguridad aplicadas contra códigos maliciosos (antivirus, antimalware, entre otros).

5.15. COPIAS DE RESPALDO DE INFORMACIÓN

Definir el procedimiento y plan de copias de respaldo de información para los activos críticos de la Entidad como infraestructura tecnológica, sistemas de información, aplicaciones, etc.

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

Se deben seguir los lineamientos establecidos para la gestión de copias de respaldo de información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información y los datos personales.

Cada Colaborador es responsable de realizar las copias de seguridad de la información y bases de datos personales en los repositorios establecido por la Agencia como son Share Point, OneDrive, y los que, por la naturaleza de los proyectos deban almacenarse en los diferentes programas o software establecidos.

La información debe almacenarse, de acuerdo con los requisitos legales, técnicos y documentales que rigen a la Agencia.

Los tiempos de preservación de las copias de seguridad deben ser definidos teniendo en cuenta los lineamientos del proceso de Gestión Documental de la Agencia Nacional Digital.

La Agencia debe asegurar la restauración de las copias de respaldo, de acuerdo con los cambios o actualizaciones tecnológicas que esto conlleve.

Se deben realizar pruebas de restauración por lo menos 2 veces al año y debe estar incluidas en el procedimiento de copias de respaldo adoptado por la Entidad, para el caso de las copias de respaldo de nube, se debe programar con el proveedor y posteriormente realizar la validación por parte del supervisor del contrato o responsable.

Para la ejecución de copias de seguridad adicionales o nuevas, el responsable de la información debe formular un requerimiento al Proceso de Gestión de Tecnologías de la Información y Seguridad y Privacidad 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.

El propietario del activo o custodio es el responsable de crear copias de seguridad de información bajo los lineamientos establecidos por la Entidad a través de los procesos de Gestión de Tecnologías de la información y Seguridad y Privacidad de la Información.

Se deben documentar las actividades desarrolladas frente al tratamiento y gestión de las copias de seguridad, con el fin de asegurar la trazabilidad de mismas.

Las copias de seguridad almacenadas en medios físicos deben contar con controles mínimos como: 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 de acuerdo con la normativa vigente.

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 mínimo una (1) vez al mes.

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 almacenada y acceso por personal no autorizado.

Los procesos de eliminación o disposición final deben cumplir con la normatividad vigente en materia de dispositivos de residuos electrónicos y conservación de información y datos.

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

Las copias de seguridad deben estar cifradas, cuando tengan información pública clasificada o pública reservada, con el fin de velar por la confidencialidad de la información.

Los empleados de planta, contratistas 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.

Los empleados de planta, contratistas o terceros de la Agencia Nacional Digital deben almacenar la información generada en sus procesos operativos, en la ubicación establecida, con el fin de asegurar la confidencialidad, integridad y disponibilidad de las copias de seguridad de cada uno de los procesos.

Los empleados de planta, contratistas o terceros son responsables de realizar la depuración de la información para optimizar los recursos institucionales.

5.16. REGISTRO Y SEGUIMIENTO Y PROTECCIÓN DE EVENTOS

En la Agencia Nacional Digital se deben registrar los eventos de procesamiento de la información.

Se deben definir, conservar y revisar o monitorear 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.

Se deben proteger las instalaciones de procesamiento de información y los registros contra amenazas externas e informáticas conforme con las políticas de seguridad física y del entorno y control de acceso.

Todos los sistemas de información de la Agencia Nacional Digital deben estar sincronizados con la hora legal colombiana, asegurando el control adecuado del procesamiento de la información en las operaciones.

Activar la auditoría a los sistemas de información de manera programada, con el fin de minimizar el impacto de las operaciones.

5.17. CONTROL DE SOFTWARE OPERACIONAL Y RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE

Se deben definir e implementar procedimientos para controlar la instalación de software en sistemas operativos.

Los equipos se deben entregar con privilegios estándar y no de administración.

Si se requiere permisos de administrador o instalación de algún software especifico en los equipos de la Agencia, por el desempeño de sus actividades laborales o contractuales, se debe realiza a través del formato de control de accesos y enviarlos al correo de seguridaddigital@and.gov.co.

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

La subdirección administrativa y financiera es la encargada de realizar la instalación de software en los equipos de la Agencia Nacional Digital y llevar el control de estos.

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

Se deben realizar revisiones periódicas mínimo 2 veces al año de la instalación de software en los equipos de la Agencia por parte del proceso de Seguridad y Privacidad de la Información y el responsable de licenciamiento.

5.18. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

La Agencia Nacional Digital establece los procedimiento y formatos para realizar una adecuada gestión de vulnerabilidades técnicas.

Se debe definir un plan de pruebas anual, el cual debe incluir mínimo dos (2) pruebas al año con retest para los activos críticos de la AND.

Los resultados de las pruebas y el seguimiento se realizan en la Matriz de gestión de Vulnerabilidades Técnicas adoptada en la entidad.

El proceso de seguridad y privacidad de la información realiza revisión de los resultados e informes de las pruebas y en conjunto con los responsables de los activos analizados se define el plan de tratamiento de vulnerabilidades técnicas, con el fin de mitigarlas y así fortalecer la seguridad de los activos.
El proceso de seguridad y privacidad 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 estas.

Todos los empleados, contratistas y terceros cuando sea el caso deben reportar oportunamente las vulnerabilidades técnicas que hayan sido detectadas al proceso de Seguridad y Privacidad de la Información al correo seguridaddigital@and.gov.co.

Se debe realizar actualización del antimalware por lo menos una vez cada 15 días en los dispositivos de cómputo y móviles o cuando sea requerido.

Los responsables de los activos de información con el apoyo del proceso de Seguridad y Privacidad de la Información deben evaluar la actualización de los parches para el entorno tecnológico, con el propósito de evitar fallas en la funcionalidad de los sistemas de información.

Se debe realizar un análisis de riesgos previo para los cambios requeridos por vulnerabilidades críticas por parte del proceso de Seguridad y Privacidad de la Información.

Se debe realizar copias de respaldo de información antes de realizar cualquier tipo de cambios en los activos y debe quedar registrado en los formatos de control de cambios establecidos.

5.19. SEGURIDAD DE LAS COMUNICACIONES

5.19.1. Gestión de la seguridad de las redes

En la Agencia Nacional Digital se protege la información que se trasporta a través de las redes de comunicación e instalaciones de procesamiento de información.

Se realiza control y gestión de acceso a las redes de comunicación, sistemas y aplicaciones, de acuerdo con las políticas de control de acceso establecidas en la Agencia.

Se aplican políticas de cifrado en el transporte y almacenamiento de la información a través de herramientas o controles tecnológicas como: firewalls, vpns, https, canales cifrados, entre otros que se consideren necesarios.

Los controles de seguridad en las redes a nivel tecnológico serán definidos por el responsable asignado por el Proceso de Gestión de Tecnologías de la Información.

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 adecuada gestión sobre el comportamiento de estas.

En la Agencia Nacional Digital se dispondrá de mecanismos de seguridad y requisitos de gestión de los servicios de red, a través del establecimiento de acuerdos de confidencialidad, nivel operativo o de nivel de servicio a nivel interno o externo cuando se contrate un Tercero.

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 estas.

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 donde se establezca el derecho de realizar auditorías cuando se requiera al proveedor sobre el servicio contratado.

Las redes de comunicación de Agencia Nacional Digital deben disponer de dispositivos de seguridad que permitan blindar y proteger la información que transita por las mismas, a través de certificados de seguridad sobre los canales de comunicación, firewalls, IPS, IDS, y/o cualquier herramienta tecnológica que mantenga la seguridad de estas.

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.

En la Agencia Nacional Digital se mantendrán separados los servicios de administración y sistemas de información de los usuarios.

La separación de redes es responsabilidad del Proceso de Gestión de Tecnologías de la Información.

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 las necesidades de las operaciones.

En la Agencia Nacional Digital se podrán 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.

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 fuertes y de acuerdo con el cumplimiento de las presentes políticas.

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 y se deben aplicar los siguientes lineamientos:

- Firmar y cumplir con los acuerdos de confidencialidad y privacidad de la información y los datos personales.
- 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.
- Contar con acuerdo de niveles de servicios.

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).

5.19.2. Transferencia de Información y acuerdos de confidencialidad

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

La Agencia Nacional Digital debe proteger la información durante su intercambio, ya sea a nivel interno o externo, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Para cualquier transferencia o intercambio de información se debe realizar a través de los lineamientos establecidos por la Agencia.

Dentro del acuerdo de transferencia o intercambio de información se debe establecer que ningún Empleados de Planta, Contratista o Terceros deben revelar o intercambiar información catalogada como pública clasificada y pública reservada, confidencial o privada, sin cumplir con el proceso formal de requisición de la información.
Para realizar la transferencia o intercambio de información se deben adoptar controles de seguridad en el transporte, almacenamiento y procesamiento.

Los intercambios de información deben estar soportados por medio de contratos, convenios o acuerdos formalizados, determinando en ellos los medios, controles en el tratamiento de la información, cláusulas de confidencialidad, entre otros lineamientos establecidos por la Entidad y las políticas de seguridad y privacidad de la información.

El intercambio o transferencia de información se debe realizar, teniendo en cuenta la normativa legal aplicable.
Se deben firmar los acuerdos de confidencialidad y privacidad de la información y datos personales con los Empleados de Planta, Contratista y Terceros cuando sea el caso.

5.20. 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 de la información y privacidad de los datos personales.

Se 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.

Se debe promover la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas y la operación de la Agencia Nacional Digital.

Se debe realizar la identificación, análisis y valoración de riesgos cibernéticos para los activos de información (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).

Realizar estudios de viabilidad para la adquisición de pólizas de seguro que pueda cubrir costos asociados a posibles ataques cibernéticos.

Se debe apoyar la gestión de continuidad del negocio para dar respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

Se 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 ciberseguridad.

Se debe monitorear continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la Agencia Nacional Digital.

La Entidad debe aplicar el *Procedimiento de Notificación y Gestión de Incidentes de Seguridad de la Información y Privacidad de los Datos Personales* cuando se presenten ciber incidentes.

5.21. USO DE SERVICIOS DE CORREO ELECTRÓNICO

La Agencia Nacional Digital establece lineamiento para asegurar un adecuado uso de la información que se procesa, transmite y almacena en el correo electrónico institucional.

Se debe hacer buen uso del correo electrónico por parte del personal de planta, contratistas y terceros cuando se el caso.

El correo electrónico institucional sólo debe utilizarse con fines laborales o contractuales.

No se debe realizar distribución de correos en cadena con contenido religioso, político, social y otros que puedan afectar la intimidad y creencias de los demás compañeros.

Una vez es asignado el correo institucional se debe realizar uso de este para todas las comunicaciones internas y externas relacionadas con las actividades laborales o contractuales.

Todo el personal de planta, contratistas y terceros cuando sea el caso debe contar con una cuenta de correo electrónica personalizada, la cual será de uso personal e intransferible.

Se podrán crear cuenta de correo genéricas para fines específicos de comunicaciones internas, externas o porque se requiera para el funcionamiento de un activo de información.

5.22. USO DE SERVICIO DE ACCESO A INTERNET

La Agencia Nacional Digital establece lineamientos de seguridad para la protección de la información y los datos en la transmisión de estos.

Todos los empleados de planta, contratistas y tercero cuando es el caso deben hacer buen uso de acceso a internet que provee la Agencia.

Está prohibido ingresar a páginas con contenido restringido como, música, películas, pornografía, juegos, entre otros que no se encuentren relacionados con el desarrollo de las actividades laborales o contractuales.

La Agencia realizará monitoreo de los accesos que se realizan por parte de los empleados de planta, contratistas y tercero cuando es el caso, con el fin de prevenir incidentes de seguridad de la información o incumplimiento de las políticas de seguridad y privacidad de la información.
Está prohibido descargar contenido restringido desde el internet institucional.

5.23. ADQUISICIÓN, DESARROLLO SEGURO Y MANTENIMIENTO DE SISTEMAS

En la Agencia Nacional Digital se establece una guía de lineamientos de desarrollo seguro de software, donde se incluyen todos los controles y lineamientos de seguridad en cada fase del ciclo de vida de desarrollo del software.

Se debe establecer una metodología de desarrollo seguro de software acorde a las necesidades de la Agencia.

Se deben definir los requisitos de seguridad y privacidad de los datos personales para todas las aplicaciones o desarrollos propios de la Agencia Nacional Digital.

Se debe activar los registros o logs de auditoría sobre el desarrollo o software.

Se debe tener controles de sesiones múltiples.

Para todos los desarrollos de sebe contar con un módulo de auditoría para sistemas de información

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

Para las transacciones de los servicios de las aplicaciones deben disponer de algunos requisitos como:

- 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.

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 la Entidad.

Se debe contar con repositorios seguros del software, protegidos con controles de acceso a través de cifrado de la información o restricciones con usuario y contraseña.
Se deben contar con control de versionamiento del software.

Se deben realizar pruebas de seguridad (estáticas y dinámicas) tipo análisis de vulnerabilidades, ethical hacking, entre otras, que permitan identificar las vulnerabilidades y así poder mitigarlas antes del paso a producción.

5.23.1. Control de cambios en sistemas de información

Los cambios en el software o sistemas de información de la Agencia Nacional Digital en los ambientes de producción deben ser gestionados conforme al *proceso de gestión de cambios* establecido.

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

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

5.23.2. 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 el ciclo de vida de desarrollo de software.

Se debe contar con repositorios seguros del código, restringidos de personal no autorizado

Todo desarrollo contratado externamente por la Agencia Nacional Digital debe ser monitoreado por el responsable o supervisor del contrato y debe contar

Se deben establecer dentro de los contratos, acuerdos o convenios cláusulas legales, técnicas, operativas y de seguridad que permitan un desarrollo seguro para la Agencia Nacional Digital.

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

5.23.3. Protección de los datos de prueba

Los datos de prueba del software en la Agencia Nacional Digital serán 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.

Todos los datos de prueba utilizados deben ser eliminados de manera segura de los ambientes de prueba.

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 estos.

5.24. RELACIONES CON LOS PROVEEDORES

En la Agencia Nacional Digital se deben definir lineamientos para la protección de los activos de información que, por la naturaleza de los contratos, convenios, etc. se deben compartir con los proveedores o terceros autorizados.

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 revisar o auditar el cumplimiento de las políticas por parte de los proveedores.

Se 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 adoptada por la Agencia Nacional Digital.

El proveedor debe diligenciar y aportar las evidencias del cumplimiento de la lista de verificación de requisitos de seguridad.

Todos los incidentes de seguridad relacionados con la ejecución del contrato con el proveedor deben ser reportados por el supervisor del contrato o quien este delegue, dando cumplimiento al procedimiento establecido.

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.

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.

Se deben identificar los proveedores y terceros críticos de la AND.

5.24.1. 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 de este.

El Supervisor del contrato debe revisar y controlar periódicamente el nivel de los servicios, cumplimiento de las cláusulas de seguridad, informes y registros generados por ellos.

Se debe realizar al menos una vez al año la revisión o auditoria a los proveedores y terceros de la AND catalogados como críticos.

5.24.2. Gestión de cambios en los servicios de los proveedores

Cualquier cambio en los servicios o ejecución de estos dentro del contrato o en los acuerdos de niveles establecidos entre las partes deben ser gestionados de acuerdo con el proceso de gestión de cambios establecido.

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

La Agencia Nacional Digital define y establece la documentación necesaria para realizar una adecuada gestión de incidentes de seguridad de la información.

La Agencia Nacional Digital establece los roles que participan en la Gestión de Incidentes de Seguridad.

Todos los empleados de planta, contratistas y terceros cuando sea el caso, deben reportar los eventos e incidentes de seguridad que detecten o se les presente a través de los canales establecidos para tal fin.
Se deben relacionar todos los incidentes de seguridad en el formato de control de eventos e incidentes establecido por la Agencia Nacional Digital, con el fin de llevar la trazabilidad de estos.

Todo el personal de planta, contratistas y terceros cuando se el caso, deben participar en la aplicación de las medidas de mitigación y planes de mejoramiento que se definan para su contención y restablecimiento de las operaciones.

Se deben definir indicadores de medición de la Gestión de Incidentes de Seguridad de la Información.

Se debe llevar el control de lecciones aprendidas de los incidentes presentados, con el fin de definir planes de mejoramiento para mitigar la probabilidad de que se vuelvan a presentar.

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 los lineamientos establecidos para la gestión de Incidentes de Seguridad.

Cualquier alteración o manipulación indebida o sin autorización de las evidencias podrá ser considerada una falta grave, el cual puede incurrir en sanciones de acuerdo con lo establecido en el manual interno de trabajo o en lo que la ley aplique.

5.26. SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

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.

En la Agencia Nacional Digital se debe planificar la continuidad de la seguridad de la información y privacidad de los datos personales determinando los requisitos que permitan proteger los activos de información frente a un evento adverso que pueda poner en riesgo las operaciones durante una crisis o desastre.

Se 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.
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.

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.

Cada Líder de Proceso en la Agencia Nacional Digital con el apoyo de los responsables de continuidad y seguridad de la información deben verificar, revisar y evaluar a través de pruebas o simulacros los planes de continuidad y controles de seguridad para asegurar la efectividad de estos 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 los lineamientos establecidos en la Agencia Nacional Digital y evaluados frente al cumplimiento de los requisitos de seguridad de la información y privacidad de los datos personales.

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 estos y el desempeño sobre los objetivos de continuidad frente a situaciones de emergencia y/o contingencia.

Se deben realizar mínimo dos (2) pruebas de continuidad a los procesos críticos de acuerdo con lo establecido en los planes de continuidad y recuperación de desastres de la AND, o cuando sea requerido por necesidad propia de las operaciones.

La Agencia Nacional Digital debe disponer de infraestructura 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.

Se deben evaluar los riesgos de seguridad de la información y privacidad de los datos personales en la continuidad de los activos de información principales de la Agencia Nacional Digital.

5.27. CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

La Agencia Nacional Digital identifica y cumple 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.

Se actualiza periódicamente el normograma de la Entidad en los requisitos de seguridad y privacidad de la información.

5.28. DERECHOS DE AUTOR Y PROPIEDAD INTELECTUAL

La Agencia Nacional Digital asegura 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".

La Agencia Nacional Digital adquiere el software solo con proveedores reconocidos en el mercado, que aseguren el licenciamiento de estos. De esta manera, en los procesos responsables son responsable de hacer la validación pertinente del proveedor de tecnología y del licenciamiento del software.

Se debe sensibilizar al personal sobre el uso del software, y licenciamiento, de tal manera que reconozca a sí mismo las implicaciones legales en caso de cualquier incumplimiento.

Se debe mantener actualizado el inventario de software con sus respectivas licencias.

Se debe controlar el uso de las licencias del software de acuerdo con las necesidades establecidas y la cantidad adquirida.

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 determinará los lineamientos pertinentes de derechos de autor y propiedad intelectual sobre toda la información (documentos, diseños, códigos fuente, bases de datos, o demás activos de información), que se generen, notificando y dejando claro a todos los usuarios dicha propiedad en los diferentes contratos o convenios establecidos. Este lineamiento será responsabilidad de los Líderes de Proceso y la Subdirección Jurídica de la Agencia.

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.

5.29. PROTECCIÓN DE REGISTROS

En la Agencia Nacional Digital se protegen 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 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 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 los lineamientos establecidos.

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 Digital podrá poner a disposición los registros a las diferentes autoridades judiciales que lo requieran para casos de investigación propia de casos que sean justificados. Así mismo, esos casos deben ser evaluados por la Subdirección Jurídica quien a su vez determinará el debido procedimiento frente a la disposición de los registros conservando el cumplimiento legal de la Agencia Nacional Digital y la protección de los datos.

Cuando sea requerido entregar registros por orden judicial, la Agencia Nacional Digital realizará dicha entrega conservando la protección de esta de acuerdo con políticas y lineamientos establecidos y acordados con el ente judicial.

5.30. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES

En la Agencia Nacional Digital se realizan revisiones a la Seguridad de la información a través de los procesos estratégicos, de evaluación y control.

Se debe dejar registro de las revisiones realizadas por la alta dirección y los demás procesos que lo realicen.

Se debe realizar por lo menos una vez al año o cuando sea requerido revisión de la documentación del Sistema de Gestión de Seguridad de la Información.

Se deben realizar mínimo una (1) auditorías internas al año o cuando se requiera al Sistema de Gestión de Seguridad de la Información.

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.

El Comité Institucional de Gestión y Desempeño debe revisar el cumplimiento de la Política, apoyado de Control Interno y los Líderes de Proceso y Seguridad y Privacidad de la Información.

6. CUMPLIMIENTO

El incumplimiento de las políticas de seguridad y privacidad de la información y los datos personales podrá dar lugar a faltas disciplinarias y sanciones internas, así como a consecuencias legales, de acuerdo con la normatividad aplicable.

7. REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LOS DATOS PERSONALES

Las políticas de seguridad de la información y privacidad de los datos personales deben ser revisadas por la Alta Dirección, Control Interno, el proceso de Seguridad y Privacidad de la Información de manera anual o por demanda cada vez que sea requerido permitiendo la evaluación y mejora continua de las mismas.

8. VIGENCIA DE LA POLÍTICA

La política se revisará al menos una vez al año y se actualizará cuando se presenten cambios organizacionales, culturales, del entorno, operativos o normativos que afecten a la Entidad. Así mismo, se revisará cuando ocurran cambios de alcance que obliguen a su fortalecimiento, o de acuerdo con los resultados de las actividades de seguimiento y control definidos.

9. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	13/10/2020	Emisión del documento
2	12/08/2022	Se quita el punto 5. denominado en la versión 1 como la Política de Seguridad y Privacidad de la Información y se genera un documento independiente con esta; el punto 6 denominado en la versión 1 Organización de seguridad de la información y privacidad de los datos personales se reforma por completo y se hacen ajustes de redacción en todas las políticas.

JUAN PABLO CEBALLOS OSPINA
Director

Revisó y aprobó: Comité Institucional de Gestión y Desempeño, sesión del 12 de agosto de 2022:
Luz Stela Rojas Duran, Subdirectora Administrativa y Financiera
Maria Angélica González Russi, Subdirectora Jurídica
Jose Alfredo Ruiz Peralta, Subdirector de Servicios Ciudadanos Digitales
Luis Alberto Clavijo Cuineme, Subdirector de Desarrollo (E)

Elaboró: Jorge Alberto Camargo Barbosa, Oficial de Seguridad de la Información
Yuli Andrea Parra, Profesional líder del SGSI, contratista