Ésta Deroga la Resolución 302 de 2005;
Da alcance a la Circular 23 de 2004;
Resolución 36 de 2009;
11 de 2017 y 670 de 2017;
Memorando 2705 de 2011

PROCURADURIA
GENERAL DE LA NACION

A ésta le da ALCANCE la
Resolución 20 de 2021;
Circular 1 de 2021 (SG)

RESOLUCIÓN N° 910

(25 SEP 2019)

"Por medio de la cual se adopta la Política de Seguridad de la Información de la Procuraduría General de la Nación"

EL PROCURADOR GENERAL DE LA NACION

En ejercicio de sus funciones constitucionales y legales, en especial las conferidas en el numeral 7 del artículo 7 del Decreto de Ley 262 de 2000, y

CONSIDERANDO:

Que el numeral 7 del artículo 7 del Decreto Ley 262 de 2000, faculta al Procurador General de la Nación para expedir los actos administrativos, órdenes, directivas y circulares que sean necesarios para el funcionamiento de la Entidad y para desarrollar las funciones atribuidas por la ley.

Que la Ley 1273 de 2009 adiciona el Código Penal con el Título VII BIS denominado "De *la protección de la información y de los datos*"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Que el artículo 4 de la Ley 1341 de 2009 establece que: "*En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines: (...) 4. Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red. (...) 11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.*".

Que el Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2, corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

Que el Decreto 1008 de 2018 por el cual establece los lineamientos generales de la política de Gobierno Digital, determina en el Parágrafo del Artículo 2.2.9.1.1.2., *"La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política.*".

Que el Artículo 2.2.9.1.1.3 ibídem establece los fundamentos en los que la Política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2° y 3°

PROCURADURIA
GENERAL DE LA NACION

RESOLUCIÓN Nº 910

(25 SEP 2019)

"Por medio de la cual se adopta la Política de Seguridad de la Información de la Procuraduria General de la Nación"

de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2° de la Ley 1341 de 2009, estableciendo como cuarto principio el siguiente:

"*(...)* ***Seguridad de la Información****: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano. (...)*"

Que la Procuraduría General de la Nación establece políticas de Seguridad de la Información lo cual le permitirá tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, aprovechando de la mejor forma los activos de información con que cuenta.

Que mediante la Resolución 302 de 2005, se determinan las políticas de uso de los equipos de cómputo de la Procuraduría General de la Nación y los servicios institucionales de Correo Electrónico e Internet, el manejo, instalación y desinstalación de software y la conservación y cuidado de la información afectada.

Que mediante la Resolución 036 de 2009, se adopta el Sistema de Gestión de la Seguridad de la Información -SGSI - de la Procuraduría General de la Nación.

Que mediante la Resolución 011 del 13 de enero de 2017 se adopta, regula y controla la modalidad de teletrabajo para la Entidad.

Que mediante la Resolución 670 de 2017, la Procuraduría General de la Nación adopta el manual de políticas y procedimientos para la protección de datos personales.

Que la Procuraduría General de la Nación suscribió el Contrato de Consultoría No. 179-089 de 2018, con la firma PASSWORD CONSULTING SERVICES S.A.S., conforme al desarrollo del Concurso de Méritos No. 3 de 2018, que tuvo por objeto llevar a cabo el diagnóstico, la planificación y la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Procuraduría General de la Nación.

Que como producto de la ejecución del Contrato 179-089 de 2018, la firma PASSWORD CONSULTING SERVICES S.A.S., entregó a la Procuraduría General de la Nación la documentación relativa a las Políticas del Sistema de Gestión de Seguridad Informática alineada con los aspectos técnicos y las recomendaciones contenidas en la norma NTC-ISO/IEC-27001:2013.

Que el Objetivo de control A.5.1.1 Políticas para la seguridad de la información, del dominio A5 Políticas de Seguridad de la Información, del Anexo A de la norma NTC-ISO/IEC 27001:2013, establece que:

PROCURADURIA
GENERAL DE LA NACION

RESOLUCIÓN N° 910

(25 SEP 2019)

"Por medio de la cual se adopta la Política de Seguridad de la Información de la Procuraduría General de la Nación"

"Se *debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.*"

Que en consecuencia de lo anterior, la Procuraduría General de la Nación adopta el documento de Políticas de Seguridad de la Información, en el cual se establecen las directrices requeridas para la implementación de un Sistema de Gestión de Seguridad de la Información confiable y flexible, y a su vez define el marco básico que guía la implantación de cualquier requisito, proceso, procedimiento, y/o acción, relacionados con la Seguridad de la Información.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO.- OBJETO: Adoptar la Política General de Seguridad de la Información para la Procuraduría General de la Nación, y las Políticas específicas de Seguridad de la Información, las cuales se anexan y hacen parte integral del presente acto.

ARTÍCULO SEGUNDO: COMUNICACIÓN: Por la Secretaría General de la Procuraduría General de la Nación comunicar la presente resolución a todos los servidores de la Entidad.

La Oficina de Prensa prestará el apoyo que se requiera para realizar la divulgación de las Políticas de Seguridad de la Información.

ARTÍCULO TERCERO. VIGENCIA Y DEROGATORIA: La presente Resolución rige a partir de su publicación y deroga la Resolución 302 de 2005.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE. 25 SEP 2019

FERNANDO CARRILLO FLÓREZ
Procurador General de la Nación

Revisó: Efraín Alberto Becerra Gomez / Secretario General
Guillermo Gómez Gómez / Jefe Oficina de Sistemas
Orlando Benavides Santacruz / Oficina de Sistemas
Edna Julieta Riveros González / Jefe Oficina Jurídica (E)
Alonso Pio Fernandez Angarita / Despacho del Procurador General de la Nación
Proyectó: Juan José Cárdenas Jiménez / Oficina de Sistemas

Anexo: Documento de Políticas de Seguridad de la Información en 42 folios

PROCURADURIA
GENERAL DE LA NACION

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN –SGSI

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCURADURÍA GENERAL DE LA NACIÓN

INTRODUCCIÓN

La Procuraduría General de la Nación – PGN tiene la responsabilidad de contar con un direccionamiento estratégico en materia de seguridad informática. El desarrollo de Políticas de Seguridad de la Información le permite a la Entidad tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, permitiendo una gestión oportuna y efectiva aprovechando de la mejor forma los activos con que cuenta.

La referencia principal para el desarrollo de una política corporativa de Seguridad de la Información orientada al desarrollo de mejores prácticas de gestión, es el conjunto de normas NTC/ISO 27000, los modelos y guías generados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

Para esto la PGN se basa en una gestión de riesgos realizada a todos los procesos de la Entidad, con el fin de prevenir que se materialicen, y poder proteger los activos de información.

Por lo anterior, la PGN define las políticas de Seguridad de la Información, con el fin de atender estos nuevos requisitos, orientadas a la prestación de servicios de calidad, que administren los riesgos cambiantes en el ámbito de la gestión de la información y de las nuevas Tecnologías de la Información y las Comunicaciones (TIC).

1. OBJETIVOS

1.1. Objetivo general

Establecer lineamientos de seguridad de alto nivel que permitan que los activos de información de propiedad de la PGN, sean accedidos sólo por las personas autorizadas que tienen necesidad legítima para la realización de las funciones propias de la Entidad (confidencialidad), que no se realicen modificaciones sin autorización y se salvaguarde su exactitud y completitud (integridad), y que sean accesibles y utilizables cuando éstos se requieran para el desarrollo de las actividades propias de la Entidad (disponibilidad); alineados con la misión, visión, objetivos estratégicos y valores corporativos de la PGN.

1.2. Objetivos específicos

Los objetivos específicos de las políticas de Seguridad de la Información en la PGN son:

a) Definir los fundamentos para el Sistema de Gestión de Seguridad de la Información (SGSI).
b) Proteger la imagen, los intereses y el buen nombre de la Procuraduría General de la Nación.
c) Reducir el nivel de riesgo en Seguridad de la Información.
d) Constituir la base para la implementación y ejecución efectiva de controles que velen por la seguridad de la información.
e) Identificar los canales de comunicación que le permitan a la Alta Dirección de la PGN mantenerse informada de los riesgos y uso inadecuado de los activos de información, así como las acciones tomadas para su mitigación y corrección.
f) Promover una cultura organizacional orientada a la Seguridad de la Información.
g) Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas de la Entidad.
h) Definir la conducta esperada en el acceso, uso y manejo de los activos de información.
i) Propender por la disponibilidad de los activos de información, servicios e infraestructura tecnológica.
j) Asegurar la continuidad en los procesos de la PGN permitiendo el cumplimiento de los objetivos estratégicos de la Entidad.

2. ALCANCE

Las políticas de Seguridad de la Información establecen las directrices requeridas para la implementación de un Sistema de Gestión de Seguridad de la Información confiable y flexible, y definen el marco básico que guiará la implantación de cualquier requisito, proceso, procedimiento, y/o acción, relacionados con la Seguridad de la Información.

Estas políticas aplican a todos los funcionarios, contratistas y terceros que tengan acceso a los servicios de red, aplicaciones y sistemas de información de la Procuraduría General de la Nación, y a las partes interesadas que accedan o hagan uso de cualquier activo de información independientemente de su ubicación, medio o formato; definen quiénes deben mantener la debida confidencialidad sobre la información de la Entidad por el tiempo que se estipule en los acuerdos establecidos.

Adicionalmente, las políticas aplican a todos los activos de información que se encuentren relacionados directa o indirectamente con el manejo de información

creada, procesada o utilizada en el soporte y desarrollo de los procesos de la Entidad.

3. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la PGN está comprometida con el desarrollo y la implementación de las políticas de Seguridad de la Información, así como de su mejora continua, mediante:

a) La autorización para la implementación de políticas de Seguridad de la Información en la PGN.
b) La revisión y aprobación de las políticas de Seguridad de la Información.
c) El suministro de los recursos necesarios para una adecuada implementación de políticas de Seguridad de la Información en el marco de la implementación del Sistema de Gestión de Seguridad de la Información.
d) La divulgación sobre la importancia en el cumplimiento de las políticas de Seguridad de la Información para el logro de los objetivos de seguridad.

El compromiso de la Alta Dirección asegura la identificación, evaluación, tratamiento, monitoreo y control de los riesgos que puedan afectar la seguridad de la Información, mediante la destinación de los recursos físicos, humanos y económicos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del Sistema de Gestión de Seguridad de la Información en los procesos productivos, misionales y administrativos.

4. GENERALIDADES

4.1. Organización de la Seguridad de la Información

La PGN mediante la Resolución 036 de 2009 adopta el Sistema de Gestión de la Seguridad de la Información -SGSI - de la Procuraduría General de la Nación, y en el artículo quinto se crea el Comité de Seguridad de la Información de la Entidad, que cuenta con las siguientes funciones:

- Proponer al Procurador General de la Nación, para su aprobación, los cambios en la Política de Seguridad de la Información y las responsabilidades generales en materia de seguridad de la información.
- Mantener informado al Procurador General de la Nación sobre el estado general de la seguridad de la información de la Entidad.
- Tener conocimiento y vigilar la investigación y el monitoreo de los incidentes de seguridad de la información por parte del Oficial de Seguridad de la Información.
- Evaluar y proponer al Procurador General de la Nación, para su aprobación, iniciativas de inversión para incrementar la seguridad de la información.
- Evaluar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

- Adoptar los indicadores de gestión de la seguridad de la información.
- Verificar que la seguridad sea parte del proceso de clasificación de la información.
- Verificar que la seguridad sea parte del desarrollo de sistemas de información o aplicaciones de software, desde las etapas tempranas del desarrollo.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Entidad y a las campañas de sensibilización en temas de seguridad de la información.

De igual forma en la Resolución 036 de 2009 se crea el perfil de Oficial de Seguridad de la Información, profesional asignado al Despacho del Procurador que tiene entre otras funciones la de liderar y coordinar la implementación de las políticas de seguridad de la información, con la participación activa de las dependencias de la Entidad.

4.2. Seguridad de los Recursos Humanos

La PGN suministrará los recursos necesarios para la formación, capacitación y/o concienciación de los funcionarios, contratistas y/o terceros con acceso a la información, en temas relacionados con la Seguridad de la Información, con el propósito que puedan identificar y reportar de manera oportuna los incidentes de Seguridad de la Información, y de esta manera se logren disminuir las vulnerabilidades y amenazas relacionadas con el talento humano.

4.3. Integridad

La PGN establecerá los lineamientos que permitan que todos los funcionarios, contratistas y/o terceros que tengan relación contractual con la Entidad y tengan acceso a la Información efectúen un manejo integral de la información interna y externa.

4.4. No Repudio

La PGN establecerá los lineamientos requeridos para garantizar la participación de las partes en una comunicación, a través de la trazabilidad, retención, auditoria y el intercambio electrónico de Información gestionada por los funcionarios, contratistas y/o terceros de la Entidad.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La siguiente es la política de Seguridad de la Información establecida para la Procuraduría General de la Nación, así:

"La Procuraduría General de la Nación representa a los ciudadanos ante el Estado Colombiano, reconoce la importancia de identificar y proteger sus activos de

información, asegurando su confidencialidad, disponibilidad e integridad, comprometiéndose a establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información enmarcado en el cumplimiento del ordenamiento legal y en concordancia con la misión, visión, objetivos estratégicos, valores y principios de la Entidad".

Conformada por más de 4 mil servidores, la Procuraduría General de la Nación tiene autonomía administrativa, financiera y presupuestal en los términos definidos por el Estatuto Orgánico del Presupuesto Nacional. Es su obligación velar por el correcto ejercicio de las funciones encomendadas en la Constitución y la Ley a servidores públicos y lo hace a través de sus tres funciones misionales principales función preventiva, función de intervención, función disciplinaria y en aras de propender por la Seguridad de la Información tiene como finalidad permitir que los activos de información de propiedad de la PGN reciban los niveles de protección adecuados de acuerdo a su confidencialidad, disponibilidad e integridad.

La Alta Dirección de la PGN, deduciendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos; alineado con el ordenamiento jurídico y normativo en concordancia con la misión, visión, objetivos estratégicos y valores de la Entidad.

Para la PGN, la protección de la información busca la disminución del impacto generado sobre los activos de información por los riesgos identificados de manera sistemática; con el propósito de mantener un nivel aceptable de exposición que permita responder por la confidencialidad, disponibilidad e integridad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

5.1. Objetivo general del SGSI

Definir en la Entidad lineamientos de acuerdo a lo establecido en el alcance; teniendo en cuenta los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI determinadas por las siguientes premisas:

a) Minimizar el riesgo a niveles aceptables definidos por la Entidad.
b) Establecer las políticas, procedimientos e instructivos en materia de Seguridad de la Información.
c) Cumplir con los principios de Seguridad de la Información: confidencialidad, disponibilidad e integridad.
d) Proteger los activos de información de la Entidad.
e) Fortalecer la cultura de Seguridad de la Información en los funcionarios, usuarios, terceros y contratistas de la PGN.

f) Asegurar la continuidad del negocio en la Entidad frente a incidentes de seguridad de la información.
g) Apoyar la innovación tecnológica.

La PGN ha decidido definir, implementar, operar y mejorar de forma continua un SGSI, soportado en lineamientos claros alineados a las necesidades de la Entidad y sus requerimientos regulatorios.

5.2. Principios de seguridad

A continuación, se establecen los principios de seguridad que soportan el SGSI de la PGN:

Las responsabilidades frente a la Seguridad de la Información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas y/o terceros.

a) La PGN protegerá la información generada, procesada o resguardada por sus procesos, infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a cada uno de los funcionarios, contratistas y/o terceros.
b) La PGN protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a su uso indebido. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
c) La PGN protegerá las instalaciones de procesamiento de información y la infraestructura tecnológica que soporta sus procesos críticos.
d) La PGN implementará controles asociados a la operación de sus procesos misionales propendiendo por la seguridad de la infraestructura tecnológica.
e) La PGN implementará controles de acceso a los activos de información, de acuerdo con su nivel de clasificación.
f) La PGN incorporará la seguridad como parte integral del ciclo de vida de los sistemas de información, a través de una adecuada gestión de riesgos.
g) La PGN propenderá por la disponibilidad de sus procesos misionales, la continuidad de sus servicios y la mejora efectiva de su modelo de seguridad, con base en el impacto que pueden generar los incidentes de Seguridad de la Información.
h) La PGN propenderá por el cumplimiento del ordenamiento legal establecido.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La PGN considera la información como un activo fundamental, razón por la cual es necesario establecer un marco normativo para asegurar que la información es protegida, independientemente de la forma en que ésta sea generada, manejada,

procesada, transportada o almacenada. Así mismo, en la Entidad se reconoce la importancia de la implementación de Políticas de Seguridad de la Información, con el fin de mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y asegurar la confidencialidad, disponibilidad e integridad de la información.

Las políticas específicas de Seguridad de la Información, constituyen un eje fundamental del Sistema de Gestión de Seguridad de la Información de la Entidad, se consideran la base para la implementación de los controles, procedimientos y estándares definidos y serán revisadas periódicamente, para que en caso de cambios relevantes en la Entidad que incidan en la Seguridad de la Información, sigan siendo adecuadas y ajustadas a las recomendaciones de la Guía de Seguridad y Privacidad de la Información establecida por MINTIC y la Norma NTC-ISO-IEC 27001.

6.1. POLÍTICA DE CONTROL DE ACCESO

OBJETIVO

La Procuraduría General de la Nación establece los lineamientos, procedimientos, responsabilidades y mecanismos de control de acceso físico y lógico, en los sistemas de procesamiento de información de acuerdo con los niveles de clasificación de los activos de información, con el fin de protegerlos de accesos no autorizados.

POLÍTICA

La Oficina de Sistemas de la PGN establece los procedimientos de creación, modificación, cancelación y reactivación de usuarios de red, de los sistemas de Información, y de lo pertinente con el Centro de Procesamiento de Datos, para controlar la asignación de los derechos de acceso a los usuarios de los recursos de la Entidad, teniendo en cuenta los requisitos de la Entidad y los niveles de seguridad lógicos y físicos requeridos.

En la presente política se definen las condiciones sobre las cuales los usuarios tienen acceso a la red, a los sistemas operativos, al acceso al Centro de Procesamiento de Datos y los aplicativos de la PGN.

Para el acceso remoto o local a la red de datos de la PGN se debe seguir lo estipulado en el procedimiento *PRO-GT-AI002 Procedimiento para el acceso a la red de datos.*

RESPONSABILIDADES

ACCESO A LA RED

La Oficina de Sistemas de la PGN es la responsable de establecer los controles de autorización y gestión, así como las prioridades de acceso y uso de los activos informáticos de propiedad de la PGN por parte de los usuarios internos y externos, para proteger el acceso a las conexiones, aplicaciones y servicios de red.

- El acceso a la red por parte de terceros debe estar estrictamente restringido y permitido únicamente con previa autorización de la Oficina de Sistemas.
- La gestión de contraseñas para el acceso a la red de la PGN se realiza por medio de la mesa de servicio, quien asigna a un funcionario para la gestión de la solicitud según la necesidad y autorización correspondiente.
- La Oficina de Sistemas implementa controles de autenticación adicionales en redes inalámbricas para controlar el acceso, por la vulnerabilidad de interceptación e inserción en el tráfico de información de este tipo de redes.
- La Oficina de Sistemas restringe los tiempos de conexión con el propósito de brindar seguridad especialmente a las aplicaciones y lugares calificados como críticos y/o de alto riesgo, por medio de uso de espacios de tiempo predeterminados y uso de sesiones interactivas de corta duración.

ACCESO POR VPN

La Oficina de Sistemas de la PGN brinda la tecnología de acceso por VPN para que funcionarios y contratistas puedan ingresar a la plataforma tecnológica de la Entidad desde una ubicación remota y de esta forma gestionen las soluciones o servicios a su cargo. Se utilizará una VPN cuando se necesite acceder a información confidencial de manera remota, y la red que se esté utilizando no ofrezca las suficientes garantías de seguridad.

Para conceder el acceso a la VPN el funcionario o contratista debe diligenciar el formato de solicitud para la creación, de acuerdo con el tipo de acceso requerido. Una vez el formato es aprobado por la Jefatura del área de sistemas, se configura el acceso y se envían las credenciales para realizar las pruebas respectivas.

El acceso a la VPN se deberá realizar con el aplicativo cliente de la página web del fabricante del dispositivo Firewall de seguridad perimetral en su última versión y bajo la supervisión de la Oficina de Sistemas.

En los equipos de seguridad perimetral se deberá controlar las fechas y horarios en los cuales se tienen los accesos por este medio, y los funcionarios de la Oficina de Sistemas monitorearán su registro de forma periódica con el fin de ejercer los controles pertinentes a estos accesos.

En caso de ser asignado un dispositivo token como doble factor de autenticación, este debe ser reintegrado en similares condiciones de su entrega a la Oficina de Sistemas al momento de completarse el servicio, finalizar el contrato o retiro del funcionario de la Entidad, siguiendo el procedimiento de entrega y devolución de token establecido para este fin.

SEPARACIÓN EN LAS REDES

- La red interna de la PGN cuenta con una segmentación lógica y física que agrupa los elementos de red con los siguientes segmentos: red LAN separada en diferentes segmentos de LAN virtuales que contienen los dispositivos de oficina, estaciones de trabajo y dispositivos de conexión inalámbrica; también existen segmentos para telefonía, equipos activos de red, administración de equipos para infraestructura, administración de equipos de seguridad perimetral y la red de Servidores.
- Las redes grandes se dividirán en dominios lógicos separados, protegidos cada uno por un perímetro de seguridad y definidos con base en evaluación de riesgos y en los requisitos de seguridad de cada uno.

INGRESO A LA RED CORPORATIVA

- La gestión de los usuarios para el ingreso a la red corporativa de la Entidad se realiza a través del Directivo Activo de Windows Server.
- El ingreso a la red corporativa se encuentra protegido, mediante el inicio seguro de sesión; los funcionarios tendrán acceso a la red corporativa en función de la operación; así mismo, es de su responsabilidad cumplir las Políticas de Seguridad de la Información, establecidas para el acceso a los sistemas de información de la Entidad.
- Se definen las medidas necesarias mediante configuraciones físicas o lógicas con las cuales se pueda brindar acceso temporal a una red confinada a los visitantes o contratistas, la cual permite tener acceso únicamente a la red pública.

INGRESO AL CENTRO DE PROCESAMIENTO DE DATOS (CPD)

- El centro de procesamiento de datos CPD de la PGN es una zona restringida y deberá contar con un control de acceso físico apropiado para asegurar que sólo se permita el acceso a personal autorizado.
- En caso que un contratista y/o proveedor requiera el ingreso al CPD deberá estar acompañado en todo momento por un funcionario de la Oficina de Sistemas.
- Todo acceso al CPD debe estar motivado
- El control y seguimiento del acceso al CPD está normado bajo el procedimiento *PRO-GT-AI-009 Procedimiento de control de acceso físico al Centro de Procesamiento de Datos CPD.*

GESTIÓN DE ACCESO A USUARIOS

Con el fin de evitar el acceso no autorizado a los sistemas operativos, la PGN hace uso de medios de seguridad que permiten la autenticación de usuarios,

realizar el registro de intentos exitosos y fallidos de autenticación, de privilegios especiales, emisión de alarmas de seguridad y en caso de ser necesario restringir el tiempo de conexión de los usuarios.

- La PGN aplica el principio de menor privilegio posible, que consiste en que sólo se otorgan los permisos necesarios para la ejecución de las funciones. Por tal motivo, el Jefe de la dependencia dueña de la información es el responsable de autorizar formalmente los privilegios (permisos) o niveles de acceso correspondientes a las cuentas de los usuarios autorizados.
- Cada una de las cuentas de acceso se compone de un nombre de usuario o "*username*" y una contraseña o "*password*". El nombre de usuario se determina por la primera letra del nombre más el apellido del usuario, y la contraseña es generada por cada uno de los usuarios.
- El superior inmediato (Jefe de área o Coordinador) es quien debe realizar la solicitud de creación o asignación del usuario a las aplicaciones que requiera el funcionario.
- Aquellas cuentas de usuario redundantes no serán otorgadas a otros usuarios; de igual manera el responsable asegurará que los proveedores del servicio solo permitan el acceso a los usuarios autorizados de acuerdo a lo establecido en el *Procedimiento de gestión de cuentas de usuario de sistemas de información PROG-GT-AT-014.*
- La Entidad asegura que los proveedores del servicio no otorguen acceso hasta que el usuario esté autorizado.
- Para los perfiles de usuario se debe considerar los roles que desempeñan cada uno de los funcionarios, conforme a las actividades propias de su labor.

REVISIÓN Y RETIRO DE LOS DERECHOS DE ACCESO A USUARIOS

- Se debe realizar la declaración formal y escrita de los derechos de acceso con firma del usuario del entendido de las condiciones y sanciones a que haya lugar en caso de acceso no autorizado.
- Los funcionarios asignados como administradores de los aplicativos, serán los responsables de controlar los derechos de acceso a los usuarios (lectura, escritura, modificación y eliminación).
- Los derechos de acceso a usuarios se revisan periódicamente. Si se presentan cambios en los roles y/o responsabilidades de los funcionarios, estos deben ser modificados por parte del administrador técnico del aplicativo.
- La eliminación, bloqueo o retiro de acceso a usuarios en el caso de funcionarios: en vacaciones, licencias o terminación de contrato laboral se realiza por medio del *formato de Solicitud de requerimientos REG-GT-AT-001.*
- En caso de retiro definitivo de un funcionario de la Entidad, al momento de realizar la entrega de todos los equipos, herramientas y elementos para que cumpliera con la labor encomendada, se realice un entrega formal de todas

las claves que el funcionario tenga asignadas tanto como las de acceso a la red, correo electrónico, aplicaciones de uso particular por su función o cualquier otra clave o dispositivo de autenticación que hubiere tenido bajo su manejo y custodia.

RESPONSABILIDADES DE LOS USUARIOS

Los funcionarios de la Entidad, terceros y/o proveedores tienen la responsabilidad de adherirse a esta política de Seguridad de la Información, y en caso que se determine un acceso lógico inadecuado que ponga en riesgo algún aspecto del SGSI, se puede constituir una falta y se aplicarán las sanciones pertinentes.

Cuando los funcionarios, contratistas y/o proveedores de la PGN evidencien algún tipo de evento o incidente relacionado al acceso lógico, debe ser informado de manera oportuna a la Oficina de Sistemas para que se tomen las medidas necesarias.

GESTIÓN DE CONTRASEÑAS

Se refiere al grado de concienciación del usuario para gestionar de modo eficiente su información en lo referente a la correcta creación de las contraseñas que ha de utilizar en los procesos y operaciones que requieren de su autenticación.

Para gestionar correctamente la seguridad de las contraseñas, y con el fin de evitar el acceso no autorizado a los sistemas informáticos, se recomienda a los usuarios tener en la cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

ACCIONES PARA CONSTRUIR CONTRASEÑAS SEGURAS

- La longitud de las contraseñas debe ser mínimo de ocho (8) caracteres.
- Las contraseñas utilizadas por los usuarios de la PGN deben cumplir con los siguientes requerimientos:
  - Contener caracteres alfabéticos como letras mayúsculas (A-Z) y minúsculas (a-z)
  - Contener caracteres numéricos dígitos del 0 al 9.
  - Cuando el sistema lo permita, se deben incluir caracteres especiales como por ejemplo @ ! # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /
- Se recomienda utilizar en una misma contraseña caracteres alfabéticos, caracteres numéricos y caracteres especiales.
- Es recomendable que las letras alternen aleatoriamente entre mayúsculas y minúsculas.
- Se debe elegir una contraseña que sea de fácil recordación.
- Contraseñas para dispositivos móviles. se deber habilitar para su ingreso y bloqueo de forma automática o manual una contraseña de acceso al dispositivo (patrón, clave numérica, reconocimiento facial o dactilar, o el que

tenga habilitado el sistema operativo del dispositivo) y en caso de ser un patrón numérico, éste será una contraseña de mínimo cuatro números.

- Generación de claves seguras: Uno de los métodos más práctico de creación de claves es el uso de mnemotecnias a partir de frases, por ejemplo: "es mejor un pájaro en mano que cien volando", se toman las iniciales de cada palabra para formar un acrónimo, que daría como resultado "emupemqcv", luego se cambian algunas letras por números, para este caso la letra "e" por un "3" y la "c" por una "@" y se obtiene la siguiente palabra "3mup3mq@v", para agregar un grado más de complejidad se cambian algunas de las letras por mayúsculas, se toma la letra "m" para obtener "3Mup3Mq@v", y se puede agregar al final un carácter especial "#", para que finalmente se obtenga "3Mup3Mq@v#", una clave robusta difícil de descifrar, que no se encuentra en un diccionario y que a pesar de que alguien más esté utilizando la misma frase, esta es una contraseña personalizada de la que seguramente nadie más sabrá los cambios que se realizaron.

RESTRICCIÓN DE USO DE CONTRASEÑAS

- Cuando se entrega el nombre de usuario al funcionario, se debe proveer una contraseña inicial segura temporal, la cual deberá ser modificada por solicitud automática ante su primer ingreso.
- Las contraseñas temporales deben ser seguras y entregadas a los funcionarios de forma que obliguen su cambio en el primer uso. Se debe evitar, en lo posible, la entrega de la clave a una tercera persona.
- Las contraseñas asignadas por el fabricante y que vienen en los sistemas y software, deben ser modificadas posterior a su instalación.
- Las contraseñas utilizadas para el acceso a los equipos de cómputo y sistemas informáticos de la PGN no deben utilizar cadena de caracteres duplicados, nombre de usuario del equipo, iniciales de la Entidad, iniciales del nombre del funcionario, número de identificación, fechas de nacimiento o cualquier otro dato personal, conjuntos de letras o caracteres de fácil identificación, o secuencias básicas del teclado (ejemplos: qwerty, abcd1234, Pgn2019, 987654, etc.).
- Hay que evitar utilizar solamente números y letras mayúsculas o minúsculas.
- No se deben utilizar palabras que se contengan en diccionarios en ningún idioma.
- Una vez la contraseña es creada, esta debe ser memorizada. Es recomendable no enviar nunca la contraseña por correo electrónico o en un mensaje. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- No se deben dejar las contraseñas escritas en un papel en lugares accesibles, ni tampoco se deben guardar en documentos de texto o legibles dentro del propio equipo de cómputo o dispositivo móvil.

- No se debe utilizar la característica de "Recordar Contraseña" existente en los exploradores (Firefox, Internet Explorer, google chrome).
- No se debe usar la misma contraseña que utiliza en la Entidad en otras cuentas como Gmail, Live, Yahoo, entre otras.
- Se debe evitar utilizar la misma contraseña en todos los sistemas o servicios.
- Se debe procurar limitar el número de intentos de acceso y que el sistema se bloquee si se excede el número de intentos fallidos permitidos.

La PGN además de las contraseñas para verificar la identidad de los usuarios, utiliza otros medios de autenticación como dispositivos biométricos y Tokens, según la sensibilidad de la información a proteger, el acceso físico protegido o los procesos a desarrollar.

PRIVACIDAD DE LAS CONTRASEÑAS

La contraseña de acceso a los equipos de cómputo y sistemas de información de la PGN de cada usuario es personal e intransferible, por tanto, cada usuario se compromete a no revelar, prestar, transferir y difundir sus contraseñas de acceso.

ROBO O PÉRDIDA DE LAS CONTRASEÑAS

En caso de presentarse un caso de robo o pérdida de contraseñas, o si el usuario sospecha que su contraseña pueda estar comprometida, es necesario solicitar el restablecimiento y cambio de ella. Este proceso debe realizarse con los administradores técnicos de cada plataforma, y en el caso de los sistemas operativos, se deben ejecutar las funcionalidades para su cambio inmediato. Conforme se recupere el control de las cuentas, se debe cambiar las contraseñas por otras más seguras. Si las páginas validan preguntas de seguridad, deben ingresarse nuevas preguntas, que servirán para otras ocasiones.

PERIODICIDAD DE LAS CONTRASEÑAS

Las contraseñas de acceso a los equipos de cómputo, dispositivos móviles y sistemas de información de la PGN, deberán ser cambiadas cada 30 días por el usuario sin permitir su reutilización. Al terminar el ciclo de vida útil de una contraseña, los usuarios deben cambiar su contraseña por una nueva.

6.2. POLÍTICA DE USO DE EQUIPOS DE CÓMPUTO

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos para el correcto uso de los equipos de cómputo pertenecientes a la Entidad.

POLITICA

Los recursos informáticos son suministrados por la PGN a los funcionarios con el único fin de desarrollar las actividades relacionadas a su cargo y al contexto de la Entidad, de acuerdo a los criterios establecidos en el Manual específico de funciones y de requisitos por competencias laborales MF-MC-00-001 de la Entidad, por lo cual estos recursos deben ser utilizados de forma adecuada y eficiente.

Es responsabilidad de los funcionarios, hacer buen uso del equipo de cómputo asignado, así como la conservación, integridad y contenidos de la información que se encuentran en los discos duros de los equipos de cómputo de escritorio y portátiles.

RESPONSABILIDADES

USO DE LOS EQUIPOS DE CÓMPUTO Y CONSERVACIÓN Y CUIDADO DE LA INFORMACIÓN CONTENIDA EN ELLOS

Los bienes y recursos de cómputo de la PGN son herramientas de apoyo a las labores y a las responsabilidades de los funcionarios y se encuentran afectados a la función pública; por ello, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, los servidores de la Entidad, al utilizar los equipos de cómputo deben observar y cumplir las siguientes directrices de uso:

- Los bienes y recursos de cómputo institucionales se emplearán de manera exclusiva por el funcionario al cual han sido asignados y únicamente para el correcto desempeño de su empleo, cargo o función; por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.
- Durante la jornada laboral y en todo tiempo de uso, corresponde al funcionario prestar la debida custodia y cuidado a los equipos de cómputo asignados, así como impedir su sustracción, destrucción, ocultamiento o utilización indebida.
- Los bienes y recursos de cómputo institucionales no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los equipos de cómputo o que vayan en contravía de las Políticas de Seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, práctica de juegos en línea, acceso a páginas musicales o de videos vía streaming, uso permanente de redes sociales personales y conexión de periféricos o equipos que causen molestia a compañeros de trabajo.
- La contraseña, clave o password de acceso es de carácter estrictamente personal e intransferible; por lo tanto, los funcionarios no deben revelarla a

terceros ni utilizar claves ajenas, siguiendo las directrices determinadas en la *Política de control de acceso*.

- Todo funcionario debe verificar que los equipos de cómputo asignados se encuentren debidamente conectados a fuentes de corriente reguladas. No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multitomas a las mismas.
- Ningún equipo de cómputo puede estar expuesto a factores externos que comprometan su integridad, tales como humedad, humo y polución.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los equipos de cómputo asignados.
- Sobre los equipos de cómputo no deben ubicarse elementos pesados, equipos electrónicos o teléfonos celulares.
- Todos los aplicativos o programas del computador se deben cerrar si el funcionario no los está utilizando o no está presente en su puesto de trabajo.
- Para evitar el bloqueo o la lentitud del equipo, es recomendable no abrir de manera simultánea varias ventanas de un mismo programa, o mantenerlas innecesariamente abiertas.
- Los únicos funcionarios autorizados para realizar modificaciones a la configuración original de los equipos, así como para destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los funcionarios de la Oficina de Sistemas y/o las personas por ellos autorizadas.
- No está permitido introducir en los equipos de cómputo elementos ajenos a su naturaleza o funcionalidad, así como ningún tipo de unidad de almacenamiento de información portátil como CD´s, DVD´S o memorias USB que estén físicamente dañadas o que no hayan sido revisadas previamente con el programa antivirus licenciado por la Entidad.
- La única dependencia autorizada para trasladar los equipos de cómputo de un puesto a otro es el Grupo de Almacén e Inventarios, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de dicha Coordinación.
- Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada de inmediato a la División de Seguridad por el funcionario que tenga a cargo el equipo.
- Los equipos se deben apagar correctamente en las ausencias prolongadas y al final de la jornada laboral.
- Todo problema de orden técnico con los equipos debe ser reportado a la Oficina de Sistemas a la mayor brevedad posible.

INFORMACIÓN CONTENIDA EN LOS EQUIPOS DE CÓMPUTO

Sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, los funcionarios al utilizar los equipos de cómputo deben observar las siguientes directrices respecto de la información contenida en los mismos:

- Mantener en reserva la documentación e información que por razón de sus funciones conserven bajo su cuidado o a la cual tengan acceso; evitarán su sustracción, destrucción, ocultamiento o utilización indebida; se abstendrán de alterarla, falsificarla, ocultarla o borrarla, e impedirán que terceros no autorizados ejecuten tales acciones sobre la misma.
- Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descargado de Internet o de cualquier red externa, debe ser escaneado con el programa antivirus licenciado de la Entidad antes de ser instalados o accedidos.
- Todos los archivos provenientes de equipos externos a la PGN, deben ser revisados para detección de virus antes de su utilización dentro de la red de la Entidad.
- Solicitar periódicamente copias de seguridad de los archivos importantes que para el cumplimiento de sus funciones, se encuentren en el disco duro del computador. *Ver Procedimiento de Copias de Seguridad*
- En el disco duro del computador únicamente puede almacenarse información de orden Institucional vigente y/o necesaria para el correcto desempeño de las funciones asignadas en la PGN.
- Todo funcionario es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible, en cumplimiento de la *Política de control de acceso.*
- En ausencia prolongada del funcionario usuario del equipo, éste bloqueará la sesión de forma manual o automática con el propósito de que la información contenida no sea expuesta a terceros, sea alterada o se le dé uso indebido.
- Todo ingreso a la Entidad de equipos de cómputo no institucionales deberá ser autorizado por el Jefe de la respectiva dependencia destino. La Oficina de Sistemas será informada para la ejecución de los debidos procedimientos de seguridad informática y la autorización de conexión a la red de datos institucional.

INSTALACIÓN Y DESINSTALACIÓN DE SOFTWARE Y HARDWARE

Sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, los funcionarios, al utilizar los equipos de cómputo deben observar las siguientes directrices respecto del uso, instalación y desinstalación de software y hardware:

- Solamente está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Oficina de Sistemas.
- Las únicas personas autorizadas para instalar o desinstalar software y hardware en los equipos de cómputo de la Procuraduría General de la Nación son los funcionarios de la Oficina de Sistemas y/o las personas por ellos autorizadas.

- En ningún caso se permite la instalación ni la actualización de software a través de enlaces webs o correos cuyo origen no sea completamente seguro.
- El software instalado en los equipos debe estar correctamente actualizado
- Está prohibido instalar, ejecutar y/o utilizar programas o herramientas de software o hardware que:
    - Adivinen las contraseñas alojadas en las tablas de usuarios de Equipos locales o remotos.
    - Monitoreen la actividad de los sistemas informáticos de equipos locales o remotos. Se excluye de esta prohibición las herramientas de software y hardware que utilice la Oficina de Sistemas con el único propósito de administrar la funcionalidad y la seguridad de los recursos informáticos institucionales.
    - Rastreen vulnerabilidades en sistemas de cómputo (hardware o software). Se excluye de esta prohibición las herramientas que utilice la Oficina de Sistemas con el único propósito de evaluar la seguridad de los recursos informáticos institucionales.
    - Exploten alguna vulnerabilidad de un sistema informático para acceder a privilegios que no han sido explícitamente otorgados por el administrador de la red o de un recurso informático en particular.
    - Tengan un carácter de juego y/o pornografía.
    - El software y hardware instalado en los equipos de cómputo de la PGN no debe ser utilizado con propósitos ilegales, no autorizados, personales o ajenos a la misión de la Entidad.
    - La Oficina de Sistemas es la única dependencia autorizada para realizar copia de seguridad del software licenciado por la Entidad, el cual no debe ser copiado o suministrado a terceros.

Para hacer cumplir esta política la PGN debe contar con:

- un listado del software autorizado
- un repositorio del software autorizado
- las claves de activación, números de serie, licencias, etc.

Para conocer el software legal del que dispone la Entidad, La Oficina de Sistemas debe llevar un registro actualizado del licenciamiento. En dicho registro se almacenará al menos la siguiente información:

- nombre y versión del producto
- autor
- fecha de adquisición
- vigencia de la licencia
- tipo de licencia
- número de usuarios permitidos por licencia
- número de licencias adquiridas por cada software

- ubicación física del producto

Periódicamente, la Oficina de Sistemas efectuará la revisión de los programas y aplicativos utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados se considera como una violación a las Políticas de Seguridad de la Información de la Entidad.

CONFIGURACIÓN, ACTUALIZACIÓN Y MANTENIMIENTO DEL EQUIPO DE CÓMPUTO

- Es responsabilidad de la Oficina de Sistemas la actualización de versiones de software y el mantenimiento de los equipos de cómputo.
- Aquellos equipos de cómputo que se identifiquen como una posible vulnerabilidad de la red de la PGN, serán aislados hasta tanto se evalúen los riesgos correspondientes y se tomen las acciones correctivas del caso, siguiendo las directrices establecidas en el *Procedimiento de gestión de incidentes de seguridad de la información.*
- Todos los equipos de la PGN tendrán instalado como mínimo: el sistema operativo, el software antivirus, la solución de mesa de ayuda y las herramientas ofimáticas que la Entidad haya definido como estándar.
- La configuración y seguridad local del equipo de cómputo será implementada de forma centralizada desde el servidor que tiene la función de controlador de dominio.

SEGURIDAD DEL SISTEMA OPERATIVO

Estarán bajo custodia de la Oficina de Sistemas los medios magnéticos o electrónicos (DVDs, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso; adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información y aplicativos.

USO DE EQUIPOS NO CORPORATIVOS

Si ese utilizan equipos de cómputo de uso público, se debe evitar realizar actividades de alto riesgo (como el uso del correo electrónico de la Entidad, trabajar con documentos online, acceder a redes sociales, realizar transacciones en los bancos online o compras online). En todo momento hay que desconfiar de la seguridad del equipo y sus conexiones. En cualquier caso que se requiera su uso por necesidad, y que implique el uso de aplicativos o usuarios de la Entidad, y no se pueda hacer uso de una conexión VPN, se recomienda:

- Revisar el entorno para evitar la mirada de observadores o de cámaras.
- Utilizar el modo de navegación privada del navegador.
- Digitar la URL o dirección web, en lugar de utilizar el buscador.

- Verificar que la página a la que se ingresa es auténtica, que utiliza el protocolo https:// y que tiene un certificado digital vigente.
- Evitar que el navegador guarde las contraseñas.
- Borrar el historial de navegación y las cookies al finalizar la sesión en el navegador.
- No conectar memorias USB ni otros dispositivos externos.
- Revisar que no quede ningún archivo personal en el equipo.

USO DE EQUIPOS DOMÉSTICOS

- Actualizar el software de los sistemas operativos y las aplicaciones.
- Utilizar un usuario no compartido.
- Instalar, activar y mantener actualizado un programa antivirus y antimalware.
- En lo posible activar el firewall del sistema operativo.
- No instalar aplicaciones sin licencia o cuyo origen sea desconocido.

6.3. POLÍTICA DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos para el uso del correo electrónico institucional.

POLÍTICA

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios de la Procuraduría General de la Nación y en tal virtud, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, su uso debe sujetarse a las siguientes directrices:

- El servicio de Correo Electrónico de la PGN debe ser empleado únicamente para enviar y recibir mensajes de orden institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier propósito ajeno a los de la Entidad.
- Los colaboradores de la PGN son responsables de las actividades realizadas con su cuenta de correo institucional. Estas actividades deben ser con fines estrictamente laborales.
- El contenido de los mensajes debe corresponder a la *Carta de Valores de la PGN* y por lo tanto no puede ser insultante, ofensivo, amenazante, injurioso u obsceno.
- La PGN tendrá acceso a los mensajes electrónicos e información almacenada en el servidor de correo, y los mismos serán parte de las políticas de respaldo y recuperación de información de la Entidad.

- Todos los mensajes generados o manejados a través de la plataforma de correo electrónico con que cuenta la PGN, incluyendo las copias de respaldo, se consideran propiedad de la PGN.
- Al redactar mensajes se deben respetar los derechos de terceros, evitar caer en el sarcasmo o la ironía y nunca comprometer la imagen de la Institución.
- El envío de mensajes debe hacerse únicamente a los destinatarios que forzosamente estén llamados a recibirlos.
- No se deben enviar mensajes de correo electrónico a todos los funcionarios, salvo que sea un asunto oficial que involucre a toda la Entidad y cuente con la autorización de la Secretaria General o de la Oficina de Sistemas.
- Las únicas personas autorizadas para enviar mensajes de correo electrónico a todos los funcionarios de la Entidad son: El Procurador General de la Nación, el Viceprocurador General de la Nación, la Secretaria General, los Jefes de Oficina, los Jefes de División y la Dirección del Instituto de Estudios del Ministerio Público.
- Las bandejas del buzón del correo electrónico institucional deben ser revisadas periódicamente y los mensajes contenidos en ellas borrados a más tardar al quinto día de su recepción, toda vez que las carpetas están concebidas para recibir información y no para almacenarla. En consecuencia, todo archivo importante recibido en el buzón debe ser guardado en el disco duro del computador y en una carpeta creada con ese fin.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser ignorado y eliminado sin abrirlo, ya que puede contener malware, en especial si contiene archivos adjuntos (*attachments*) con extensiones .exe, .bat, .prg, .bak, .pif,, o archivos comprimidos (.rar, .zip, .arc), o que tenga referencias explícitas, por ejemplo eróticas o alusiones a personajes famosos.
- Todo mensaje tipo phishing, spam, smishing, vishing, o alguno similar, debe ser calificado como correo no deseado, eliminado, y nunca respondido.
- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de compras, deportivas, agencias matrimoniales, citas, almacenes de cadena, plataformas de pago, compras en línea, juegos, casinos, páginas de pornografía o en cualquier otra página ajena a los fines de la PGN.
- El reenvío de mensajes sólo debe realizarse en casos estrictamente necesarios.
- Sólo deben imprimirse los mensajes importantes que así lo requieran, ya que una de las ventajas y fines del servicio de correo electrónico institucional es la transmisión de información con ahorro de papel.
- Todos los archivos enviados o recibidos en la plataforma de correo electrónico deben ser vacunados previamente con el antivirus licenciado en la Entidad.

- La cuenta de correo no debe utilizarse para enviar o recibir música, programas, material pornográfico, fotos, videos o cualquier otro archivo ajeno a los fines de la Entidad.
- Está prohibido utilizar el sistema de correo electrónico institucional para el desarrollo de actividades políticas, comerciales, de entretenimiento o para la transmisión de mensajes vulgares, sexistas, racistas u obscenos.
- Se prohíbe el uso de correos electrónicos personales (en servicios como Hotmail, Yahoo, Gmail, entre otros), para el envío de comunicaciones oficiales de la Entidad, esto con el principal objetivo de gestionar el riesgo de fuga de información. Si llegase a ser necesario el uso de dichas cuentas de correo diferentes a la institucional, se debe dejar constancia de su uso para cualquier comprobación solicitada.
- No está permitido el envío y/o reenvío de mensajes en cadena, fotos, chistes, bromas, adivinanzas, material pornográfico, y en general cualquier información que atente contra el buen nombre y la moral de las personas o contra la integridad de los datos manejados por la PGN.
- Cuando se envía información sensible usando el correo electrónico Institucional, ésta deberá ir cifrada utilizando una contraseña adicional. Para este caso, la Oficina de Sistemas debe garantizar la adopción de métodos que especifiquen los controles de cifrado de información que permitan el cumplimiento del *Procedimiento para el intercambio de información segura* en cada uno de los medios utilizados, y se debe propender porque estos medios sólo sean conocidos por el emisor y por el(los) receptor(es), del mensaje.
- Al crear las cuentas de correo electrónico institucional, la Oficina de Sistemas establecerá criterios de restricción, de acuerdo con las funciones o perfil del usuario, a efectos de racionalizar la capacidad del buzón, delimitar la posibilidad de enviar mensajes colectivos o a distintos grupos, orígenes o destinatarios, entre otras medidas.
- Los funcionarios y contratistas deben enviar correos electrónicos con la respectiva firma de autoría.

RESPONSABILIDADES

La PGN tiene instalada en su infraestructura de seguridad perimetral un filtro antispam que permite que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada de los funcionarios evitando así su posible apertura. Sin embargo, en algunas ocasiones existen correos maliciosos que se filtran en la bandeja del correo institucional y probablemente contienen virus, buscan infectar los equipos con algún tipo de malware o sustraer información personal solicitando los datos de los funcionarios en alguna página fraudulenta.

En todo momento el funcionario debe considerar que el contenido del correo, asunto, remitente, origen y solicitud debe ser consistente con algún aspecto de su realidad; por ejemplo, si no se conduce un vehículo no habrá lugar a foto comparendos, o multas generadas en algún lugar del país al que nunca ha

viajado; si no tiene familiares en el extranjero no recibirá herencias de ellos; si no declara renta no le llegarán cobros de la DIAN, o si no posee una cuenta bancaria en un determinado banco no debería actualizar ningún dato en sus portales; o si no participa en rifas no habrá lugar a ganarse premios; así mismo las grandes compañías nunca regalan ni obsequian cosas por internet, ni por el reenvío de mensajes.

La prevención es lo más importante, por lo que se recomienda lo siguiente:

- No abrir ningún enlace ni descargar ningún archivo adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
- Evitar dar clic en enlaces dentro de correos de dudosa reputación o que generen zozobra (cobros jurídicos, foto comparendos, créditos en mora, fotografías de personajes famosos, cobros de la DIAN, citaciones judiciales, demandas, actualización de datos bancarios, rifas ganadas, herencias de familiares que no conoce, entre otros). Siempre se deben ignorar.
- No se debe confiar únicamente en el nombre del remitente; en lo posible hay que comprobar que el dominio del correo recibido es de confianza (el dominio es el nombre que va después del símbolo de la arroba).
- Si el mensaje recibido es de un contacto conocido y le solicita información inusual, debe contactar al remitente por teléfono u otra vía de comunicación para corroborar la legitimidad de la solicitud.
- Sospechar de los mensajes con fallas reiteradas de ortografía.
- Si no se conoce con certeza la procedencia del archivo adjunto en el mensaje, no hay que habilitar las macros de los documentos ofimáticos, incluso si el propio archivo así lo solicita.
- Nunca diligenciar datos personales, ni información financiera, ni bancaria en correos electrónicos que lo soliciten.
- No dar clic en ningún enlace sospechoso o que desconozca su procedencia.
- En caso de sospecha, se debe bloquear el remitente como correo no deseado y proceder a eliminar el mensaje de correo de la bandeja de entrada.
- Descargar o actualizar la versión más reciente del navegador utilizado para asegurar que presenta menos vulnerabilidades al momento de utilizarlo.
- Evitar ingresar a sitios web de dudosa reputación, podrían estar infectados y al entrar a la página se descarga automáticamente malware o cualquier tipo de virus.
- En lo posible, mantener actualizado el sistema operativo y el software antivirus del equipo.
- Si tiene alguna duda contactar al área de soporte técnico de la Oficina de Sistemas.
- Si al verificar archivos adjuntos se sospecha que no son válidos y que pueden contener virus, no se deben abrir, proceder a eliminar el mensaje y

a bloquear el remitente (en correo no deseado) para no recibir futuros mensajes de él.
- Seguir estas recomendaciones e informar a la Oficina de Sistemas cualquier correo irregular que llegue a la bandeja de entrada.

6.4. POLÍTICA DE USO DEL SERVICIO DE INTERNET

OBJETIVO

Establecer por parte de la Procuraduria General de la Nación los lineamientos para el uso del servicio de internet de la Entidad.

POLITICA

El servicio de Internet suministrado por la Procuraduría General de la Nación es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios; por lo tanto, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, al utilizarlo los usuarios deben observar y cumplir con las siguientes directrices:

- El servicio de Internet es provisto por la Entidad a sus funcionarios de tal forma que lo utilicen para efectos de desempeñar de mejor forma sus actividades laborales. Las actividades relacionadas con el trabajo incluyen labores de investigación, apoyo técnico y consulta profesional que puedan encontrarse via internet y que soportan la función del funcionario, por lo tanto el servicio de Internet Institucional exclusivamente debe ser utilizado para el desarrollo de actividades directamente relacionadas con el cumplimiento de la misión de la Procuraduria General de la Nación y las funciones de sus servidores.
- Los usuarios pueden acceder a la red interna (Intranet) y cualquier otro sitio de Internet que tenga relación con su actividad laboral y organizacional.
- La PGN aplica el principio de menor privilegio posible, que consiste en que sólo se otorgan los permisos necesarios para la ejecución de las funciones. Por tal motivo, el Jefe de la dependencia dueña de la información es el responsable de autorizar formalmente por medio escrito al Jefe de la Oficina de Sistemas los privilegios (permisos) o niveles de acceso correspondientes a las cuentas de los usuarios autorizados.
- Para todos los funcionarios en la Entidad se tienen habilitadas páginas de noticias, seguridad social, periódicos de circulación nacional, correos electrónicos, Entidades bancarias, consultas de la rama judicial, consultas de jurisprudencia, todas las páginas gubernamentales (.gov.co), todas las páginas educativas (.edu.co), y otras categorias generales. En caso de ser requerida alguna página diferente, el Jefe de la dependencia dueña de la información es el responsable de autorizar formalmente por medio escrito al Jefe de la Oficina de Sistemas los sitios a los cuales los usuarios autorizados pueden ingresar.

- El acceso a los servicios bancarios, servicios educativos y servicios personales que se encuentran habilitados vía Internet, podrán ser utilizados en forma mesurada en horarios en los que no se atiende al público o bien donde no existe alta demanda del enlace de datos para labores propias de la Entidad (horas no laborales).Las configuraciones de los computadores y de los navegadores es de exclusiva responsabilidad de la Oficina de Sistemas y siempre estarán orientadas a asegurar el buen uso del ancho de banda para el acceso a las aplicaciones de interés de la Entidad.
- Cada usuario será responsable por cualquier afectación no deseada que provoque al intentar visitar algún sitio no permitido o bien, instalar un programa no autorizado ni licenciado.
- Sólo los usuarios autorizados podrán realizar video conferencias de acuerdo a la descripción de sus funciones y necesidades del servicio que le corresponde.

RESPONSABILIDADES

PROHIBICIONES SOBRE EL USO DEL SERVICIO DE INTERNET INSTITUCIONAL

El servicio de internet institucional NO debe ser utilizado para:

- La instalación y/o uso de programas para descargar aplicaciones desde Internet hacia los computadores.
- La instalación de software no licenciado ni autorizado que ponga en riesgo la seguridad y estabilidad de la red, así como el cumplimiento de las normas legales sobre el uso de software legal.
- Solicitar, transmitir, o descargar cualquier información, mensaje de datos y/o aplicación informática que pueda infringir o violar los derechos de privacidad, confidencialidad y protección de datos de la Entidad y de sus servidores.
- Ejecutar o intentar ejecutar cualquier actividad con fines ilícitos como accesos no autorizados, robo, bloqueo o daño de información, sobrecarga o deterioro de los servicios informáticos, redes y sistemas de terceros.
- Suplantar o falsificar la identidad de terceros
- El acceso a las redes de tipo social (Facebook, Instagram, Tumblr, Twitter, Snapchat, whatsapp, Youtube, etc.), sitios de streaming, sitios de contenido sexual, comunidades de hackers, terrorismo, descargas de software libre, descarga de videos, descarga de películas, música Online, TV Online, radio Online o descargas de contenido en línea en general, y otras que la Entidad considere inapropiadas. En caso de requerirse estos accesos, el Jefe de la dependencia dueña de la información es el responsable de autorizar formalmente por medio escrito al Jefe de la Oficina de Sistemas los privilegios (permisos) o niveles de acceso correspondientes a las cuentas de los usuarios autorizados.

- Enviar o recibir archivos de video, audio, texto, fotos, etc., con contenidos insultantes, ofensivos, injuriosos, obscenos o violatorios de los derechos de autor.
- Enviar o descargar archivos de video, audio, texto, fotos, etc., no propios del cumplimiento de los propósitos institucionales o de las funciones laborales.
- Escuchar música conectado directamente al sitio en Internet que provee este servicio o mediante el acceso directo a un equipo de la red local institucional.
- Instalar o ejecutar archivos o software de procedencia desconocida.
- El uso de aplicativos de mensajería o chats con fines personales
- Acceder a sitios de pornografía, juegos o apuestas.
- Realizar llamadas internacionales personales.
- Vulnerar o intentar vulnerar la seguridad de la plataforma tecnológica de la PGN.
- Ejecutar actividades con el propósito de afectar de cualquier forma los intereses, la imagen, y el prestigio de la Entidad, así como, divulgar en páginas de Internet de cualquier tipo de información falsa que pueda afectar a la ciudadanía o al bien público.
- Utilizar del servicio Institucional de Internet con cualquier otro propósito particular o personal, tomándose el nombre de la Institución.
- Se prohíbe cualquier tipo de transmisión vía Internet que no esté autorizada.

La conexión a Internet no debe realizarse directamente desde la línea telefónica, dispositivos tipo USB, u otro medio de conexión existente, salvo expresa autorización de la Oficina de Sistemas.

En los puestos de trabajo donde aplique, la conexión a Internet siempre debe cerrarse o desconectarse cuando no se esté navegando.

La Oficina de Sistemas está habilitada para limitar el acceso a determinadas páginas de Internet, establecer los horarios de conexión, supervisar los servicios ofrecidos por la red, autorizar la descarga de archivos y verificar cualquier otra petición relacionada con la navegación para el cumplimiento de los fines institucionales.

Los canales oficiales de la Procuraduría General de la Nación presentes en redes sociales se mantendrán habilitados para su consulta y divulgación. En caso de observarse altas mediciones en el ancho de banda institucional, la Oficina de Sistemas podrá restringir su acceso hasta tanto se normalice el servicio.

CONTROLES POR EL MAL USO DEL SERVICIO DE INTERNET INSTITUCIONAL

Es función de la Oficina de Sistemas el control del tráfico de internet en los equipos institucionales, mediante los dispositivos de seguridad perimetral. Este tráfico podrá ser registrado y eventualmente revisado con el fin de determinar los accesos no permitidos y establecer las acciones correctivas a que haya lugar.

La revocación del servicio institucional de Internet, es una medida de prevención contra el uso no permitido o mal uso y que puedan afectar los niveles de servicio o atentar contra los principios y valores institucionales.

El Jefe o superior inmediato será informado sobre el mal uso que se le está dando al servicio de Internet por los funcionarios de su área.

En caso de comprobarse el reiterado uso indebido del servicio de internet, se pueden revocar al funcionario los permisos de navegación asignados.

6.5. POLÍTICA DE CONTROL DE MALWARE

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación normas para el control de virus y otros tipos de malware que se puedan presentar en los equipos y dispositivos de cómputo, con el fin de minimizar los riesgos de pérdida de información y su afectación en los activos de información de la Entidad.

POLÍTICA

La PGN dispone de forma permanente de una plataforma antimalware con la cual se facilita la detección de amenazas que puedan afectar los activos de información de la Entidad.

RESPONSABILIDADES

La Oficina de Sistemas de la PGN es responsable de determinar qué tipo de solución es la más conveniente para la Entidad, seleccionando la más apropiada de entre las disponibles en el mercado, considerando los activos informáticos, servicios actuales, compatibilidad con la infraestructura y la versatilidad de la plataforma.

La Oficina de Sistemas de la PGN es responsable de instalar el sistema antimalware en cada dispositivo de cómputo y en los servidores; debe utilizarse únicamente este software licenciado para la revisión y verificación de malware en los equipos y archivos, y los funcionarios no deben desactivar, alterar o desinstalar el aplicativo instalado para este fin.

La Oficina de Sistemas de la PGN debe garantizar la actualización permanente de la plataforma antimalware con el fin de replicar en los equipos de la Entidad las últimas firmas de búsqueda y contención de programas maliciosos.

Es responsabilidad de cada usuario utilizar el aplicativo antimalware instalado en su equipo para diagnosticar la presencia de virus o infecciones en la información que provenga de diferentes medios, tales como páginas de internet, correos electrónicos, memorias USB, discos portátiles, etc. Este proceso debe ser realizado antes de abrir o ejecutar los archivos, con el fin de no propagar virus informáticos u otros programas maliciosos al interior de la red.

Todos los medios magnéticos suministrados por un tercero deben ser revisados por el antivirus de la entidad antes que estos sean utilizados en los equipos de cómputo de la Entidad.

Cada usuario será responsable por cualquier afectación no deseada que provoque al abrir un enlace o un archivo contaminado con virus u otro tipo de malware, sin que fuese escaneado previamente con el software antimalware instalado en su equipo.

En caso que se presente una infección por ejecución de malware, el funcionario debe informar al personal encargado responsable de la Oficina de Sistemas, los cuales realizarán mínimo las siguientes acciones:

- Desconexión y aislamiento del equipo afectado
- Desinfección de los archivos, y en caso que no sea posible, la eliminación de los mismos
- Reinstalación del software o aplicativos afectados
- Registro formal del incidente en la herramienta dispuesta para este fin

Al recibir un correo con un archivo o un link adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y ésta condición no se percibe con facilidad. La descarga de archivos adjuntos maliciosos o abrir links presentes en los mensajes, podría hacer que se infecten los equipos con algún tipo de malware. Siempre se deben vacunar los archivos descargados con el antivirus de la Entidad, procurando que éste se encuentre activo y actualizado.

Estas son algunas medidas para identificar un archivo adjunto malicioso:

- Tiene un nombre que incita a descargarlo, por ser habitual o porque se cree que tiene un contenido atractivo
- El icono no corresponde con el tipo de archivo (su extensión). En este caso se suelen ocultar archivos ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.

- Tiene una extensión conocida pero en realidad está seguida de muchos espacios para que no se vea la extensión real (ejecutable), por ejemplo: listadoanual.pdf .exe
- El archivo adjunto tiene más de una extensión, por ejemplo informeanual.docx.exe
- Pide habilitar opciones deshabilitadas por defecto como el uso de macros
- Si no se reconoce la extensión del archivo adjunto puede que se trate de un archivo ejecutable (hay muchas extensiones diferentes a las usadas de forma habitual)
- Puede encubrir un archivo JavaScript (archivos con extensión .js).

Al recibir en un mensaje un enlace, antes de dar click en él se debe:

- Revisar la URL, esto se hace situándose sobre el texto del enlace para visualizar la dirección antes de hacer clic en él. Por lo general los enlaces falsos redirigen a sitios de almacenamiento en la nube como Dropbox, Onedrive, Google drive, Sharepoint, o alguno similar, en el que solicitan descargar el archivo con malware que allí se encuentra.
- No abrir las páginas desde los enlaces que llegan en los mensajes de correo. Por seguridad, siempre prefiera escribir la dirección de la página que quiere consultar en el campo de búsqueda del navegador.
- Identificar enlaces sospechosos que se parecen a enlaces legítimos fijándose en que:
  - Pueden tener letras o caracteres de más o de menos y se pasan desapercibidas, por ejemplo *www.daviviendaa.com*
  - Podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0).

6.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación normas de escritorio y pantalla limpia con el propósito de proteger documentos físicos y dispositivos de almacenamiento removibles de la Entidad, con el fin de reducir los riesgos de acceso no autorizado, fuga, perdida o daño de la información, responsabilizando de esta manera a los funcionarios sobre el cuidado de los activos de información de la Entidad.

POLÍTICA

La política de escritorio limpio conlleva la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. Por esta razón no se debe dejar información sensible a la vista de personas que pudieran hacer uso indebido de la misma. El cumplimiento de esta política conlleva, entre otras actividades, a mantener el puesto de trabajo limpio y

ordenado, guardar la documentación y los dispositivos extraíbles que no están siendo usados en el momento o al estar ausentes del puesto o al fin de la jornada laboral y a no apuntar nombres de usuarios ni contraseñas en post-it o similares. En observancia de lo anterior, los funcionarios de la PGN cumplirán con lo siguiente:

- Todos los funcionarios deben mantener los puestos de trabajo limpios y organizados, y deben contar con los implementos básicos para poder desarrollar las funciones propias de su cargo.
- Cada uno de los funcionarios debe mantener su puesto de trabajo libre de información propia de la PGN, susceptible de ser alcanzada, visualizada, copiada o utilizada por personal sin autorización.
- Todo documento, medio magnético u óptico removible que contenga información confidencial o sensible de la Entidad, debe ser almacenado en lugares seguros.
- En las áreas de atención al público, los equipos de cómputo deben situarse de forma que la información desplegada en sus monitores no pueda ser visualizada por personas externas, aplicando el bloqueo automático de protector de pantalla. La información interna debe tener el mismo tratamiento de la información confidencial o sensible.
- Al finalizar la jornada de trabajo, el funcionario o contratista debe guardar en un lugar seguro los documentos o medios que contengan información reservada, confidencial o de uso interno.
- Toda información impresa, confidencial o sensible, debe ser retirada de manera inmediata de la impresora y no se debe dejar en el escritorio sin custodia.
- El personal responsable de la Oficina de Sistemas deshabilitará por defecto los puertos USB de todos los equipos y los habilitará para aquellos usuarios que necesiten, de forma justificada y debidamente autorizada, dicha funcionalidad.

RESPONSABILIDADES

SEGURIDAD EN IMPRESORAS

El personal asignado por la Oficina de Sistemas verificará que las impresoras conectadas a la red de la Entidad cumplan con:

- Que se encuentren conectadas en los segmentos de red institucionales
- El acceso a su panel de configuración debe ser mediante contraseña y por canales cifrados
- Si están conectadas por WIFI se debe configurar su seguridad y cifrado
- Los discos duros de las impresoras deben revisarse periódicamente
- Los puertos USB de las impresoras no deben estar habilitados

- Siempre que sea posible, se debe disponer de mecanismos de impresión segura (con contraseña)
- El usuario debe recoger inmediatamente aquellos documentos enviados a imprimir

PANTALLA LIMPIA

- El funcionario debe bloquear el equipo de cómputo cuando se ausente del puesto de trabajo. Para esto se recomienda el uso de los comandos *CTRL+ALT+SUPR* y dar click en *"Bloquear"* ó *WINDOWS+L (en caso de Windows)* y los comandos correspondientes para otro tipo de dispositivos, como computadores Mac, tabletas, smart phones y otros.
- Los funcionarios no deben almacenar información sensible en el escritorio de los equipos de cómputo.
- Los equipos de cómputo deben tener aplicado el fondo de pantalla corporativo establecido por la Oficina de Sistemas.
- Todo equipo de cómputo debe poseer la configuración de bloqueo automático por inactividad. En la PGN el periodo de inactividad estará definido en 3 minutos.
- Los funcionarios deben almacenar la información de forma ordenada, haciendo uso de carpetas y jerarquías de almacenamiento.
- En lo posible los funcionarios de la PGN deben evitar el almacenamiento de: videos, fotografías o información personal en los equipos de cómputo asignados.
- Los funcionarios apagarán su equipo al finalizar la jornada laboral

6.7. POLÍTICA DE DISPOSITIVOS MÓVILES

OBJETIVO

Establecer por parte de la Procuraduria General de la Nación las normas sobre el uso de los dispositivos móviles institucionales y dispositivos móviles personales al servicio de funciones propias del cargo o función, velando por su uso adecuado, responsable y mejores prácticas en cuanto a seguridad de la información.

POLITICA

La PGN proporciona las condiciones adecuadas para el manejo de los dispositivos móviles (computadores portátiles, tabletas y teléfonos inteligentes) institucionales y personales que hagan uso de los servicios de la Entidad. Así mismo, vela porque los funcionarios hagan un uso responsable de los servicios, equipos y aplicativos disponibles en la Entidad.

La asignación de los dispositivos móviles a los funcionarios de la PGN y/o terceros (que así lo ameriten), se realiza teniendo en cuenta los procedimientos fijados por

el grupo de Almacén e Inventarios para su entrega, de acuerdo con la disponibilidad de equipos y servicios, así como la función a desempeñar.

Se autorizará acceso a la plataforma de tecnologías y sistemas de información a proveedores de servicios, que por la naturaleza de sus actividades requieran acceder a estos servicios en forma periódica, previa solicitud enviada al Jefe de la Oficina de Sistemas, o al Coordinador del Grupo de Infraestructura, por el interventor del contrato o profesional responsable de las actividades del contratista o proveedor de servicios.

La Oficina de Sistemas es responsable de gestionar la implementación y el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión, concientización y capacitación para su adecuado cumplimiento.

RESPONSABILIDADES

USO DE CONTRASEÑAS

- Todos los dispositivos móviles pertenecientes a la Entidad que se encuentren asignados a algún funcionario de la PGN y/o tercero, deben contar con credenciales de uso (nombre de usuario y contraseña o password) que limite solamente a su responsable contar con el acceso directo a la información que éste contiene.
- La gestión de las contraseñas para los dispositivos móviles debe seguir las pautas indicadas en la *Política de Control de Acceso* de la Entidad.

PROTECCIÓN FÍSICA

- Todos los dispositivos móviles de la PGN deben estar registrados, inventariados y asignados a un funcionario.
- Los dispositivos móviles asignados a funcionarios y/o contratistas son personales e intransferibles.
- En caso de pérdida o robo del equipo, el funcionario debe informar inmediatamente a la División de Seguridad quienes tomarán las medidas pertinentes.
- Los equipos asignados, en particular aquellos que almacenen información sensible, no deben ser entregados a personal ajeno a la PGN.
- El mantenimiento de los equipos portátiles queda restringido al personal delegado de la Oficina de Sistemas para realizar esta labor. Por tanto se prohibe que el usuario haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización escrita de la Oficina de Sistemas.
- En el caso de que se considere necesario instalar o activar algún software de localización se comunicará al usuario del dispositivo antes de realizar la

entrega del mismo. El usuario que va a estar geolocalizado deberá firmar un documento aceptando esta condición.

- Los equipos portátiles institucionales tendrán el acceso a la BIOS protegido con contraseña para evitar modificaciones en la configuración por parte del usuario.
- Si el usuario sospecha que el equipo o dispositivo móvil es víctima de una infección por virus u otro software malicioso, debe notificar a la mayor brevedad posible al personal técnico responsable de la Oficina de Sistemas.
- El dispositivo móvil no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes.
- El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones de la Entidad. Por tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene.

INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES

- Está prohibida la instalación de aplicaciones no autorizadas en los dispositivos móviles institucionales por parte de los funcionarios de la PGN o del tercero asignado.
- El proceso de instalación y configuración de las aplicaciones en los dispositivos móviles institucionales, sólo puede ser realizado por los profesionales designados por la Oficina de Sistemas de la Entidad.
- El aseguramiento de la administración de los dispositivos móviles, pertenecientes a la PGN, será administrado por el profesional designado por la Oficina de Sistemas de la Entidad.
- Periódicamente, la Oficina de Sistemas efectuará la revisión de los programas y aplicativos utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados se considera como una violación a las *Políticas de Seguridad de la Información* de la Entidad.

SEGURIDAD DEL SISTEMA OPERATIVO

- Para garantizar la disponibilidad, confidencialidad e integridad de la información contenida en los dispositivos móviles, el profesional designado por la Oficina de Sistemas, es quien debe otorgar los respectivos permisos.
- Los usuarios de los dispositivos móviles propenderán por la última versión (o la última estable y segura) del sistema operativo y sus aplicativos.
- Los parches o actualizaciones deberán ser obtenidos de manera formal provenientes del fabricante o desarrollador de los sistemas y aplicativos.
- Estarán bajo custodia de la Oficina de Sistemas los medios magnéticos/electrónicos (DVDs, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente

las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

SINCRONIZACIÓN DE CORREO ELECTRÓNICO EN DISPOSITIVOS MÓVILES

- La sincronización de la cuenta de correo electrónico corporativo en el equipo móvil de uso institucional debe ser configurada por los profesionales designados por la Oficina de Sistemas de la Entidad.
- Para la sincronización de la cuenta de correo electrónico corporativo en el equipo móvil de uso personal debe realizarse una solicitud a través de comunicación remitida al Jefe la Oficina de Sistemas o el Coordinador del Grupo de Infraestructura, previa autorización del Jefe directo del usuario que lo requiere.

REGISTRO DE INGRESO Y SALIDA DE LOS DISPOSITIVOS MÓVILES

Los dispositivos móviles propiedad de la Entidad, que ingresen o salgan de las instalaciones de la PGN deben ser registrados en las planillas de ingreso y salida de equipos, controladas por la empresa de vigilancia, y su registro se realizará observando los procedimientos y formatos que la División de Seguridad disponga para este fin.

DISPOSITIVOS MÓVILES DE USO PERSONAL

Corresponde a aquellos dispositivos móviles que los usuarios traen a la PGN con el objetivo de facilitar la consecución de sus actividades en desarrollo del contrato, cargo o función que desempeñan.

Estos equipos podrán unirse temporalmente a la red de datos de la PGN, de forma inalámbrica o cableada, obteniendo la configuración por defecto que los equipos de redes y seguridad tengan determinada. Para el ajuste en los niveles de navegación o la aprobación de acceso a aplicativos, debe realizarse una solicitud a través de comunicación remitida al Jefe la Oficina de Sistemas o el Coordinador del Grupo de Infraestructura, previa autorización del Jefe directo del usuario que lo requiere.

NORMAS DIRIGIDAS A TODOS LOS FUNCIONARIOS

- No dejar desatendidos los equipos o dispositivos móviles.
- No llamar la atención acerca de portar un equipo o dispositivo valioso.
- No colocar identificaciones de la PGN en el dispositivo, salvo los estrictamente necesarios.
- No colocar datos de contacto técnico en el dispositivo.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias

para evitar accesos no autorizados al dispositivo, pérdida, inadecuada manipulación o robo de estos.

- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- En lo posible no se deben sincronizar documentos confidenciales.
- Siempre se debe proteger los equipos contra malware con un antivirus.
- Se debe optar por cifrar y proteger los datos sincronizados en plataformas de almacenamiento en la nube (Google Drive, Onedrive, Icloud, etc.) con una contraseña adicional.
- Se debe usar el inicio de sesión en dos pasos cuando esté disponible.
- No deben usarse respuestas secretas que cualquier persona pueda adivinar.
- Siempre se debe cerrar la sesión de usuario cuando se esté ubicado en lugares públicos o se estén usando equipos compartidos.

MEDIDAS DE SEGURIDAD ADICIONALES PARA PROTEGER LOS DISPOSITIVOS MÓVILES

- Evitar descargar aplicaciones de sitios no reconocidos, que no estén certificados, o de sistemas operativos no avalados por el fabricante.
- Evitar abrir archivos adjuntos de correo electrónico en el teléfono, ya que pueden contener programas maliciosos.
- Evitar hacer clic en enlaces de mensajes de texto, dado que puede contener enlaces a sitios web maliciosos.
- Realizar actualizaciones de las aplicaciones ya instaladas, con el fin de disminuir las vulnerabilidades detectadas.
- Al usar un navegador en el dispositivo móvil, se recomienda seguir las mismas precauciones en el teléfono como se haría en un computador.
- Se recomienda digitar la dirección del sitio a visitar directamente en el navegador y si se da clic en un enlace hacia una nueva página, se debe comprobar la URL para asegurarse de no ser redirigido a un sitio desconocido.
- Se debe apagar la función de bluetooth de los dispositivos cuando no se esté utilizando, ya que se puede espiar las actividades del teléfono como el registro de llamadas y mensajes de texto.
- Bloquear el teléfono usando las funciones propias de esta tarea (usando patrón o clave) y activar el borrado remoto.
- Limpiar de forma regular la memoria para accesos a información personal en el teléfono.
- Instalar y mantener actualizado un software antimalware, para los equipos portátiles con el software licenciado de la PGN, y para otros dispositivos móviles en caso de no contar con un producto licenciado, con un software de las tiendas de productos de los principales fabricantes de sistemas que se encuentren en el mercado.

6.8. POLÍTICA DE TELETRABAJO

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación, las condiciones y medidas de seguridad de la información para los funcionarios con la modalidad de teletrabajo.

POLITICA

La Entidad bajo la resolución 011 del 13 de enero de 2017 adopta, regula y controla la modalidad de teletrabajo. La presente política complementa las directrices establecidas en la resolución en mención, en lo concerniente a los aspectos de Seguridad de la Información aplicables dentro del desarrollo del Teletrabajo a los funcionarios asignados.

Dentro del documento "Acuerdo de Trabajo", se consignan las obligaciones de la PGN y las obligaciones generales de los teletrabajadores, bajo la modalidad de teletrabajo, las cuales con su aceptación se darán entendidas como de obligatorio cumplimiento.

Mediante la Resolución No. 811 del 12 de diciembre de 2018, "Por la cual se establece el reglamento interno del Comité de Coordinación y Seguimiento al Programa de Teletrabajo de la Procuraduría General de la Nación" se define la conformación del comité y se determinan los funcionarios que hacen parte del mismo.

RESPONSABILIDADES

CONDICIONES DE ACCESO

- Todo funcionario con autorización de teletrabajo posee un usuario y contraseña para el acceso al equipo y los sistemas de información de la PGN.
- Las contraseñas utilizadas para la modalidad de Teletrabajo en los componentes de acceso remoto a los servidores remotos y sistemas informáticos de la PGN deben cumplir con lo pertinente definido en el capítulo de gestión de contraseñas de la *Política de control de acceso* de la Entidad.
- El soporte y mantenimiento del equipo del funcionario autorizado con Teletrabajo y trabajo remoto, se realiza por medio de la Oficina de Sistemas de la PGN.
- Los funcionarios deben reportar los incidentes de seguridad de la información que sean generados desde la función de Teletrabajo o trabajo remoto de forma inmediata a la Oficina de Sistemas de la PGN.

- Los funcionarios deben utilizar una cuenta de usuario para el entorno de Teletrabajo de la PGN y otra para los asuntos personales.
- El equipo utilizado para teletrabajo debe cumplir con estándares mínimos certificados, como lo son el tener licenciamiento para los programas que lo requieran y un programa antivirus activo y vigente, con el fin de minimizar vulnerabilidades con el uso de software no autorizado.

RESTRICCIONES

- Los funcionarios con la modalidad de Teletrabajo no deben desatender la sesión en su equipo de cómputo, ni utilizar conexiones inseguras (por ejemplo: conexiones Wi-Fi abiertas existentes en cafés internet, aeropuertos, hoteles, centro comerciales, parques públicos, entre otros); así mismo, deben dar cumplimiento en todo momento a las *Políticas de Seguridad de la Información* definidas por la Entidad.
- Toda conexión remota a la plataforma tecnológica de la Entidad se realizará mediante una arquitectura cuyo método de conexión sea segura, con equipos de cómputo previamente identificados y privados, en consecuencia con el acceso por VPN definido en la *Política de control de acceso* de la Entidad.
- La contraseña de acceso al equipo de cómputo y sistemas informáticos de la PGN de cada usuario, es personal e intransferible, por lo anterior, cada uno de los usuarios se compromete a no revelar, prestar, transferir ni difundir sus claves de acceso.

COPIAS DE RESPALDO

Las copias de respaldo o backup se deben realizar siguiendo los lineamientos de la *Política de copias de seguridad* y de los procedimientos de copia de seguridad de la PGN y debe involucrar los medios para la sincronización del equipo a la carpeta que la Oficina de Sistemas asigne.

PARA TODOS LOS FUNCIONARIOS CON LA MODALIDAD DE TELETRABAJO

- Las conexiones remotas asignadas se revisarán por parte de la Oficina de Sistemas por lo menos una vez cada seis meses con el fin de renovar al funcionario los permisos asignados.
- En caso de cambio de roles y/o responsabilidades del funcionario dentro de la Entidad, el Comité de Coordinación y Seguimiento del teletrabajo será el encargado de revisar, revocar y actualizar los respectivos accesos a la red o sistemas de información, e informar a las áreas respectivas para su actualización.
- La Oficina de Sistemas de la Entidad establecerá un procedimiento para la asignación de accesos a los entornos de Teletrabajo de la PGN, de igual manera un esquema de verificación para el licenciamiento y actualización de software en los dispositivos utilizados para Teletrabajo.

- La Oficina de Sistemas debe establecer el procedimiento y los controles de acceso para la definición de aspectos técnicos en los equipos usados, como lo son el uso de particiones cifradas, arranque dual de sistemas operativos, división de los entornos de trabajo (entorno Teletrabajo y entorno personal), etc.
- En los entornos de Teletrabajo se debe garantizar que los usuarios asignados a esta modalidad cuenten con medidas de seguridad para los equipos asignados y/o utilizados para su entorno de trabajo (como lo son la conexión por medio de una VPN, realizar las actualizaciones periódicas del sistema operativo, mantener actualizado un software antivirus, antimalware y activación del firewall del equipo de cómputo.
- El funcionario no está autorizado para realizar instalaciones de software que genere riesgos en la integridad y confidencialidad de la información, actividad que debe realizar los funcionarios de la Oficina de Sistemas, para lo cual ésta debe establecer los procedimientos para la conexión y asistencia remota que garanticen la continuidad de las operaciones, evitar cambios no autorizados, fugas de información, y el borrado remoto de la información.
- En caso de presentarse algún incidente con la información, de acuerdo con las directrices establecidas en la *Política de Gestión de Incidentes*, la Oficina de Sistemas podrá revocar los permisos del usuario informando al superior inmediato las razones por las cuales se realizó ésta acción, en todo caso manteniendo un registro de los dispositivos utilizados para el Teletrabajo y logs de accesos de los aplicativos y sistemas utilizados.
- El Instituto de Estudios del Ministerio Publico, en conjunto con el Comité de Coordinación y Seguimiento del Teletrabajo y la Oficina de Sistemas, deben capacitar a los funcionarios autorizados para el trabajo en la modalidad de Teletrabajo sobre los riesgos, conceptos, responsabilidades, cuidados de la información conforme a su clasificación, acciones y sanciones por divulgación no autorizada, protección de datos personales, y otros temas pertinentes a esta modalidad.

6.9. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

OBJETIVO

Establecer por parte de la Procuraduria General de la Nación, los lineamientos y controles necesarios para llevar a cabo una adecuada transferencia de información dentro de la Entidad y/o con partes externas, con el fin de mantener la seguridad de la información, a través de los diferentes tipos de comunicación o transferencias definidos en la Entidad.

POLITICA

La transferencia de información deberá realizarse protegiendo la confidencialidad, disponibilidad e integridad de los datos de acuerdo con la clasificación del tipo de

información involucrada. La información pública clasificada y pública reservada que se encuentre en medio impreso o físico, debe permanecer en cajones cerrados bajo llave, su entrega se dará en mano y el embalaje deberá ser suministrado con sellos de seguridad. Se aplicarán estos mecanismos de seguridad para proteger la información allí contenida.

RESPONSABILIDADES

Con el fin de garantizar la confidencialidad, disponibilidad e integridad para el intercambio de la información entre funcionarios, contratistas y terceros, en la PGN se define la transferencia de información con las siguientes condiciones:

- Para mantener la seguridad de los activos de información de la Entidad, cada supervisor del contrato firmado con un tercero, está en la obligación de verificar la firma del ACTA PARA DETERMINACION DEL ALCANCE DEL COMPROMISO DE CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACION, previa a la transferencia de información entre la Entidad y sus proveedores y/o contratistas.
- Los terceros con quienes se intercambia información sensible de la PGN deben destruir de manera segura la información suministrada, una vez ésta cumpla con la función para la cual fue enviada y demostrar a las partes interesadas la realización de las actividades de borrado y destrucción.
- En caso de intercambiar información sensible de la PGN por correo electrónico, ésta deberá ceñirse a lo establecido en la Política de uso del correo electrónico institucional.
- Las partes interesadas deben evitar tener conversaciones confidenciales sobre información sensible de la Entidad en lugares públicos, oficinas abiertas, ascensores y lugares de reunión social para evitar la escucha o interceptación de información no autorizada. Para el tratamiento de información tipo verbal, se debe tener reserva y solo comentarla en áreas o zonas seguras dentro de la Entidad.
- No está permitido el intercambio de información pública clasificada y reservada de la Entidad, por medio telefónico o por correo electrónico, sin las debidas protecciones y controles necesarios que la ameriten por su nivel de clasificación. Para tal fin, los funcionarios se pueden apoyar en soluciones tecnológicas de cifrado o asignación de claves para la información almacenada e intercambiada en medio digital.
- La información física no se debe dejar abandonada en impresoras, en el puesto de trabajo o en un área de circulación alta de personas. Por esta razón, toda la información que se reciba o envíe a través de impresoras, máquinas de fax u otros medios de reprografía y transmisión de datos, debe ser controlada, monitoreada y recopilada por el funcionario que los esté utilizando.
- El funcionario es responsable de la suscripción o diligenciamiento de formularios electrónicos a través de internet. Por lo tanto, debe evitar el diligenciamiento de los datos de ubicación física, teléfonos móviles,

teléfonos fijos, estructura organizacional, divulgación de cargos o información sensible de la Procuraduría General de la Nación.

- El funcionario custodio de la información de cada Oficina o Dependencia, es el responsable de velar por el cumplimiento de la clasificación, foliación y rotulación de los documentos, de conformidad con los términos ordenados por la Secretaría General, el Grupo de Archivo o quien haga sus veces.
- Para el envío de información pública clasificada o pública reservada a otra Entidad, se debe tener autorización escrita del Jefe de grupo, Coordinador, o superior inmediato, y se debe hacer transferencia de la reserva; por tal motivo cada funcionario se responsabiliza de la información que entregue sin cumplir estos controles.
- Los proveedores y terceros deben cumplir con las políticas de seguridad de la información, que tengan algún tipo de relación con la transferencia de información en medios físicos.
- Todo correo electrónico y/o medio físico con destino a terceros que contenga información confidencial y/o reservada, en caso de estar cifrado no debe tener ningún contenido en el cuerpo del correo que haga referencia a la clave de acceso. Esta contraseña podrá ser suministrada a través de contacto telefónico y/o correo electrónico posterior a su envío sin ningún adjunto.
- Ningún colaborador de la PGN puede establecer o configurar redes de área local, conexiones remotas a redes internas o externas o intercambiar información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información, empleando la infraestructura de red de la Entidad, sin la previa autorización de la Oficina de Sistemas.

6.10. POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS Y GESTION DE LLAVES CRIPTOGRÁFICAS

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos para garantizar que se hace un uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad, autenticidad y el no repudio de la información sensible manejada por la Entidad, tanto almacenada como en tránsito.

POLITICA

La información sensible y confidencial que se maneja en la PGN:

- bases de datos, registros de usuarios, correos electrónicos confidenciales
- información sujeta a protección legal
- backups
- información confidencial en dispositivos extraíbles y móviles

- credenciales de acceso
- credenciales para pagos online
- sistema de gestión documental

Por su trascendencia e importancia debe estar especialmente protegida tanto en tránsito como cuando está almacenada. Para proteger esta información, además de controlar el acceso a la misma y proteger los sistemas con los que la manejamos, en la Entidad se utilizan herramientas criptográficas que cifran los datos, haciéndolos ilegibles por aquellos que no dispongan de la clave de cifrado. De esta manera se garantiza la confidencialidad e integridad de la información sensible cuando está almacenada.

Como parte de la estrategia de Gobierno en Linea, la Oficina de Sistemas de la Procuraduría General de la Nación, en aras de tener una gestión pública efectiva, eficiente y eficaz, adquirió el Sistema de Información de Gestión Documental Electrónico de archivo (SIGDEA), el cual en el componente de no repudio de datos requiere los siguientes certificados, a los que se les debe garantizar la continuidad a fin de no afectar la operatividad del sistema:

- Certificado Digital de Persona Jurídica.
- Certificado de Servidor Seguro (SSL).
- Correo Electrónico Certificado.
- Estampado Cronológico.

Con el fin de brindarle seguridad y garantizar la continuidad y no afectar la operatividad del sistema SIGDEA la Procuraduría General de la Nación, adquirió los Certificados de Servidor Seguro, Certificado de Firma Digital Persona Jurídica y Correo Electrónico certificado. Estas técnicas criptográficas permiten firmar digitalmente los documentos y correos electrónicos relevantes, lo que garantiza además la autenticidad y no repudio de los mismos. También el sistema usa mecanismos de estampado cronológico, que se aplica con todos los documentos que se reciben, radican, digitalicen y son firmados digitalmente dejando constancia de fecha y hora de la transacción.

La PGN como ejecutora del Presupuesto General de la Nación, a través de la División Financiera, se encuentra en obligación de gestionar y registrar las transacciones presupuestales y financieras a través del Sistema Integrado de Información SIIF Nación, mediante el uso de firmas digitales para ingresar a dicho Sistema. Por esta razón para poder operar el sistema SIIF Nación se requiere que el usuario disponga de un certificado digital que permita firmar digitalmente las transacciones que en dicho sistema se registran. Para que la Entidad cumpla con los parámetros operativos, técnicos y de seguridad que en dicho sistema se han establecido, suministra certificados digitales a todos los funcionarios usuarios que en la Entidad consultan y registran operaciones presupuestales y financieras en este aplicativo.

La Procuraduría General de la Nación tiene instalados Certificados de Servidor Seguro SSL, para la seguridad de los aplicativos, la plataforma de comunicaciones unificadas, el servicio de correo institucional y servicios web y sus servidores, con lo cual los usuarios de la página web, el correo electrónico y los sistemas de información tienen la certeza que están ingresando a sitios oficiales de la Procuraduría con un canal seguro y que sus transacciones, servicios, consultas y trámites se están realizando con la debida protección.

RESPONSABILIDADES

Para establecer el sistema de cifrado, se tiene en la cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente.

Los propietarios de los activos individuales sobre los cuales se aplican controles criptográficos, son los responsables por la correcta aplicación de los controles criptográficos particulares.

Las llaves criptográficas se deben proteger contra pérdida, modificación, destrucción no autorizada y divulgación, por lo tanto, es necesario tener en cuenta las siguientes medidas:

- Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- Definir el protocolo para activar y recibir las llaves y su distribución a los usuarios autorizados y el periodo de activación de la misma.
- Definir criterios para el almacenamiento de las llaves y la forma de acceso por parte de los usuarios autorizados.
- Definir criterios para el cambio o actualización de las llaves.
- Revocar las llaves cuando se han puesto en peligro o cuando se retira el funcionario de la Entidad.
- Definir criterios para archivar las llaves y para destruirlas.
- Definir procedimiento para recuperar llaves pérdidas o corruptas.
- Mantener registros de auditoría de las actividades de gestión de llaves
- La caducidad de las llaves criptográficas públicas de los terceros será potestad de ellos y acogida por la PGN
- Sera responsabilidad del tercero actualizar sus llaves criptográficas públicas e informar a la Entidad para su actualización.
- Cuando la PGN haga uso de un control criptográfico asociado a firmas digitales, se tendrá en cuenta la legislación pertinente que describe las condiciones bajo las cuales la firma digital es legalmente obligatoria.

GENERACIÓN DE LLAVES

La información que contenga contraseñas de usuario, llaves o claves para el control de acceso a los sistemas de información catalogados como sensibles no pueden ser almacenadas en texto plano. Es responsabilidad de la Oficina de Sistemas utilizar y/o definir los algoritmos de cifrado más apropiados para ser utilizados en los sistemas de información críticos, con base en un análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad, no repudio así como las tecnologías de cifrado disponibles para tal efecto.

El software de cifrado genera una primera clave de forma aleatoria al momento de su instalación y el usuario del equipo asigna una segunda clave.

Los computadores portátiles de la Entidad deben contar con una herramienta de cifrado, con el fin de proteger la información almacenada en los discos duros de estos equipos, salvaguardando así la confidencialidad de la información almacenada.

Todos los funcionarios que tengan a su cargo equipos portátiles deben al momento de asignar la clave al software de cifrado tener en cuenta las condiciones para la asignación de contraseñas de acuerdo a los lineamientos establecidos en la Política de control de acceso.

ALMACENAMIENTO

El software de cifrado se almacena local y temporalmente en el disco del equipo portátil.

ACCESO A VPN CON CANALES CIFRADOS

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre estos puntos usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de la red pública. La forma más sencilla de establecer esta comunicación en Internet, se realiza mediante una VPN (Red Privada de Datos), en la que los paquetes viajan encriptados, y mediante técnicas de autenticación se asegura que el emisor y el receptor que están intercambiando información reciban los datos correctos sin ser alterados.

Los usuarios que solicitan el acceso externo a los recursos de la red deberán realizarlo mediante un canal VPN, que permita su autenticación en los sistemas internos y que use tecnologías de encriptación, mediante el envío de paquetes seguros para la red pública.

6.11. POLÍTICA DE COPIAS DE SEGURIDAD

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos de copias de seguridad con el fin de mantener los principios de confidencialidad, disponibilidad e integridad de la información de la Entidad.

POLITICA

La PGN adoptará prácticas de Copias de Respaldo o Backup para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido de los sistemas de información.

RESPONSABILIDADES

RESPALDO DE LA INFORMACIÓN

La PGN tiene procedimientos de Copias de Respaldo o Backup y procedimientos de restauración de los datos que se almacenan en los equipos servidores de la Entidad, para mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de la misma.

Los procedimientos de respaldo y restauración incluyen:

- Determinar el nivel de criticidad de la información y el periodo de retención de las copias de respaldo.
- Registros exactos y completos de las copias.
- Extensión y frecuencia de los respaldos, que indique los requisitos de seguridad de la información y la importancia de la operación.
- El tipo de copia de seguridad estimando los recursos y tiempo necesarios para llevarlas a cabo:
    - completa: se copian todos los datos a un soporte;
    - incremental: sólo se graban los datos que han cambiado desde la última copia;
    - diferencial: se copian los datos que han cambiado desde la última copia completa.
- El respaldo de información confidencial debe protegerse por medio de cifrado.

Para el respaldo seguro de la información, la PGN adoptó el "*Procedimiento de copias de respaldo de la información*".

Para recuperar la información almacenada en las copias de respaldo, la PGN diseñó el "*Procedimiento de restauración de copias de respaldo de información*".

Las copias de respaldo deben ser restauradas (probadas) con regularidad para comprobar su adecuado almacenamiento y así evitar pérdida de información y garantizar la continuidad de negocio.

Para el almacenamiento interno y custodia de las copias de respaldo de la información, la Entidad cuenta con una cintoteca ubicada en el Centro de Procesamiento de Datos (CPD). Para el almacenamiento y custodia externos, la PGN realizará contratos con empresas de seguridad especializadas en el tema, para el transporte y custodia de la información sensible. Los controles aplicados a los medios en la sede principal se extenderán para cubrir el sitio donde está el respaldo.

Las herramientas automatizadas para facilitar el respaldo y restauración de la información adquiridas por la PGN deberán probarse suficientemente antes de la implementación y a intervalos regulares, por el administrador de la herramienta.

Cada uno de los empleados será el responsable de resguardar la información crítica y sensible dentro de los recursos asignados para tal fin, como es el caso de carpetas compartidas, medios de almacenamiento externo u otros elementos de almacenamiento.

Es responsabilidad de la Oficina de Sistemas:

- Realizar en forma adecuada y periódica las copias de respaldo de la información que esté bajo su custodia.
- Establecer la frecuencia de las copias de la información, de acuerdo con la criticidad de los datos almacenados. En todo caso, por mejores prácticas deberán realizarse mínimos dos copias de respaldo, una se conservará en la cintoteca del centro de cómputo de la PGN y la otra deberá permanecer fuera de las instalaciones de la Entidad. Se exceptúan aquellos archivos de información que provienen de Entidades externas, o que en razón de cambios en la tecnología no puedan ser duplicados. Las solicitudes para entrega de información por parte del custodio externo deben ser tramitadas con la debida autorización del jefe de Sistemas.
- Mantener actualizadas las versiones de las aplicaciones en el medio de almacenamiento utilizado en su momento, de forma que le permita atender requerimientos operacionales internos y legales.
- Verificar de forma constante por los operadores del centro de cómputo la ejecución correcta de las copias de respaldo, suministrar las cintas requeridas para cada trabajo de copia, controlar la vida útil de cada cinta o medio y el procedimiento de limpieza de la unidad de grabación.
- El administrador de las bases de datos realizará pruebas periódicas de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas adaptado para tal fin, con el objetivo de garantizar que las cintas se encuentran adecuadas para una eventual restauración.
- Los medios que vayan a ser eliminados deben ser destruidos para garantizar que no quede información remanente en los mismos. Esto debe responder a procedimientos o guías para la eliminación segura de la información.

Es responsabilidad de los funcionarios de la Entidad:

- Almacenar la información sensible de la PGN en los equipos o medios de almacenamiento que la Oficina de Sistemas disponga para tal fin, para que la misma pueda ser respaldada.
- Ningún tipo de información que se refiera a la misión de la PGN debe ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en las carpetas de archivos que la Oficina de Sistemas disponga para tal fin.
- El dueño de la información es responsable de definir los periodos de retención y la frecuencia con que se hacen las copias de respaldo, para garantizar la continuidad de su operación y la consulta histórica de su información.
- Los funcionarios pueden compartir información y archivos a través de recursos compartidos del sistema operativo, previa solicitud realizada a la Oficina de Sistemas y cada dependencia debe mantener depurada la información de las carpetas compartidas, como mejor práctica para la optimización de uso de los recursos que entrega la Entidad a sus funcionarios.

IMPLEMENTACION AGENTES DE COPIAS DE RESPALDO O BACKUP

Conforme al contrato 179-070-2017 cuyo objeto fue: "Seleccionar al oferente que entregue a título de compraventa a la Procuraduría General de la Nación los elementos de software, hardware y servicios conexos necesarios para la implementación de una solución de backup para los datos de los sistemas informáticos de la Procuraduria, a partir de la infraestructura de almacenamiento y archiving que se encuentra actualmente instalada en la Entidad", la Entidad adquirió durante el año 2017 una Solución de Backup de la marca Hitachi, administrada por el Software CommVault, junto con los servicios conexos de implementación, soporte y garantía.

Dentro de la fase de implementación del proyecto, se contó con el asesoramiento de un Ingeniero del fabricante Hitachi, quien adelantó el despliegue de los agentes de backup sobre los diferentes servidores de la Entidad, a fin de generar las correspondientes copias de seguridad.

En total fueron desplegados 94 agentes de backup, de acuerdo a la siguiente tabla:

AGENTES INSTALADOS

TIPO	APLICACIÓN	AGENTES	SUBTOTAL
Database	MySQL	3	20
	Oracle	4	

	PostgreSQL		2	
	SQL		11	
Directory Service			2	2
Exchange	Archiver		2	8
	Database		4	
	Mailbox		2	
Distributed Apps			6	6
Granular Agents	File System	NAS	2	52
		Unix	7	
		Windows	43	
	Virtual Server		6	6
TOTAL				**94**

De acuerdo a los distintos ambientes existentes en la Entidad, se definieron las siguientes políticas en la herramienta:

NOMBRE DE LA POLÍTICA	DESCRIPCIÓN
DB_ARCH	Archiving de correo electrónico
DB_ORA_SQL	Bases de datos: Oracle, SQL, PostgreSQL; MySQL
EndPoint	Usuarios finales PC
FS_APP	File system y Aplicaciones
Vmware_NAS	Máquinas virtuales y NAS

AGENDAMIENTO DE RESPALDOS O BACKUPS

Teniendo en cuenta la ventana de backup definida por la Entidad (7pm – 6am) y la duración promedio de las copias de seguridad, se agendaron los respaldos de la siguiente manera:

HORA	SUBCLIENTE	FULL	INCREMENTAL	DIFERENCIAL	SYNFULL
10 -11 am.	Exchange DB	semanal (domingo)			
12 - 01 pm.	EndPoint	mensual (último viernes)	semanal (l-m-mc-j)		semanal (viernes)

HORA	SUBCLIENTE	FULL	INCREMENTAL	DIFERENCIAL	SYNFULL
04 - 05 pm.	Oracle DB	mensual (últ. domingo)			
05 - 06 pm.	Oracle DB				semanal (domingo)
06 - 07 pm.	Unix	mensual (últ. domingo)			
07 - 08 pm.	Exchange DB		semanal (l-m-mc-j-v-s)		
07 - 08 pm.	Unix				semanal (domingo)
08 - 09 pm.	Vmware	diario			
09 - 10 pm.	Unix		semanal (l-m-mc-j-v-s)		
10 - 11 pm.	SQL DB	semanal (domingo)		semanal (l-m-mc-j-v-s)	
11 - 12 am.	Oracle DB		semanal (l-m-mc-j-v-s)		
12 - 01 am.	Win - AD	mensual (últ. domingo)			
01 - 02 am.	Win - AD		semanal (l-m-mc-j-v-s)		semanal (domingo)
02 - 03 am.	Backup copy	diario			
05 - 06 am.	SQL Log - MySQL PostgreSQL	diario (repite c/ 4 hrs)			
06 - 07 am.	Oracle Arch	diario (repite c/ 4 hrs)			

RESTAURACION DE COPIAS DE RESPALDO O RESTORE

El funcionario y/o contratista de la PGN que requiera de un archivo o información a restaurar, deberá realizar la solicitud directamente al Administrador Software de Backup del Grupo de Infraestructura por medio de correo electrónico.

Con el fin de mantener la integridad y disponibilidad de la información, las copias de respaldo se colocan a prueba mediante la restauración aleatoria de algún archivo al que se le haya realizado la copia de respaldo. Si la restauración del backup es exitosa, se documenta en la bitácora de respaldo.

6.12. POLÍTICA DE DESARROLLO SEGURO

OBJETIVO

Establecer por parte de la Procuraduria General de la Nación los lineamientos de Seguridad de la Información dentro del ciclo de vida de desarrollo de software.

POLITICA

La PGN establecerá e implementará un conjunto de lineamientos y controles para garantizar la Seguridad de la Información durante todo el ciclo de vida de los desarrollos realizados por terceros a los sistemas de información de la Entidad.

Para la PGN es importante asegurar la confidencialidad, disponibilidad, integridad y no repudio de la información que se encuentra almacenada en los diferentes sistemas de información, por esta razón se considera que para todas las fases del ciclo de vida de desarrollo de software se deben incluir requisitos de seguridad, y estos deben ser obligatorios, con el fin de minimizar vulnerabilidades que podrían aparecer en caso de no implementar planes de seguridad al desarrollo realizado.

RESPONSABILIDADES

En todas las fases del ciclo de vida de desarrollo de software los proveedores deben tener en cuenta los siguientes requisitos de seguridad:

- Se deben identificar, justificar, acordar y documentar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software.
- Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
- El cambio de versionamiento en el ambiente de producción debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso que se deba dar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
- Se deben realizar pruebas de seguridad en el ambiente de pruebas, con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.
- Los ambientes de desarrollo, pruebas, capacitación y producción, deben estar separados.
- Los usuarios y/o terceros que están involucrados en esta instancia, deben utilizar perfiles diferentes en el ambiente de desarrollo, pruebas y producción; además, asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente.
- El ambiente de prueba debe simular el ambiente de producción. Sin embargo los datos de prueba utilizados, a pesar de corresponder a una estructura similar a la de producción, deben utilizarse traslapados, para garantizar la seguridad y protección de los datos.

- En caso de requerirse hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información se encuentra enmascarada o anonimizada, con el fin de que no se llegue a comprometer la confidencialidad.

COMPROMISO CON EL MEJORAMIENTO CONTINUO

Cuando los supervisores de los contratos de los proveedores relacionados con desarrollo de software, evidencien una oportunidad de mejora con respecto a los servicios prestados por dichos proveedores en cuanto al ciclo de vida de desarrollo de software, esta debe ser informada de manera oportuna a los funcionarios responsables de la Oficina de Sistemas con el fin de analizar y tomar las medidas pertinentes.

SANCIONES

Los proveedores de la PGN, que tenga a su cargo el desarrollo de software, tienen la obligación de cumplir con las *Políticas de Seguridad de la Información* establecidas por la Entidad. Cualquier incumplimiento a las mismas que pueda poner en riesgo algún aspecto del SGSI constituye una falta que puede ser penalizada de acuerdo con la normatividad vigente.

6.13. POLÍTICA DE GESTIÓN DE INCIDENTES

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos de gestión de incidentes de seguridad de la información, incluyendo los mecanismos para registrar los incidentes con sus pruebas y evidencias, con objeto de estudiar su origen y evitar que ocurran en un futuro, con el fin de mantener los principios de confidencialidad, disponibilidad e integridad de la información de la Entidad.

POLITICA

La PGN adoptará prácticas de gestión de incidentes de seguridad de la información con el fin de identificarlos, gestionarlos, tratarlos y mitigarlos, para de esta forma mantener la confidencialidad, integridad y disponibilidad de la información sensible de la Entidad, cumpliendo con las directrices de las normas ISO 27001:2013 y el estándar ISO 27035 sobre gestión de incidentes de seguridad.

RESPONSABILIDADES

Entre los distintos tipos de incidentes de seguridad, se pueden destacar los siguientes:

- incidentes no intencionados o involuntarios
- daños físicos
- incumplimiento o violación de requisitos y regulaciones legales
- fallos en las configuraciones
- denegación de servicio
- acceso no autorizado, espionaje y robo de información
- borrado o pérdida de información
- infección por código malicioso.

Las gestión de los incidentes de seguridad de la información involucran las fases de reporte, análisis, evaluación del impacto, escalamiento, aplicación de las acciones definidas, recolección de la información, comunicación de la gestión realizada a los interesados y revisión de los incidentes con mayor impacto y recurrencia, con el fin de tomar acciones para reducir la probabilidad e impacto de los incidentes de seguridad de la información en el futuro. Para ejecutar correctamente un plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

La política de gestión de incidentes de seguridad de la información está enfocada a:

- Detectar, reportar y evaluar incidentes de seguridad de la información.
- Responder a incidentes de seguridad de la información, incluida la activación de controles adecuados para la prevención y la reducción de impactos.
- Reportar las vulnerabilidades de seguridad de la información, evaluarlas y tratarlas adecuadamente.
- Aprender de los incidentes y vulnerabilidades de seguridad de la información, implementar controles preventivos y hacer mejoras al enfoque global para la gestión de incidentes de seguridad de la información.

Es responsabilidad de los funcionarios, contratistas, terceros y proveedores:

- Reportar al grupo de soporte del área de Sistemas, cualquier incidente de seguridad de la información identificado.
- Cumplir con las políticas de seguridad de la información definidas por la PGN.

Es responsabilidad del grupo de soporte al usuario:

- Gestionar los incidentes de seguridad de la información reportados por los funcionarios, contratistas, terceros y proveedores.
- Aplicar las acciones correctivas necesarias para mitigar y reducir el impacto de los incidentes de seguridad de la información presentados.

- Comunicar a las partes interesadas la gestión realizada y los planes de tratamiento aplicados.

CRITERIOS DE EVALUACIÓN DEL IMPACTO DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

El siguiente cuadro presenta la definición de los niveles en los que deberán ser clasificados los incidentes de seguridad que se puedan presentar en la PGN y que tengan algún nivel de afectación en la confidencialidad, disponibilidad e integridad de la información en sus diferentes estados:

Clasificación del nivel de la gestión de incidentes para la PGN

NIVEL	RANGO	DESCRIPCIÓN	AFECTACIÓN PORCENTUAL DE LA OPERACIÓN
5	Grave	La materialización del evento tiene efectos graves dentro de los procesos de la PGN catalogándose como un incidente grave.	80% A 100%
4	Alto	La materialización del incidente tiene altos efectos dentro de los procesos de la PGN.	60% A 80%
3	Medio	La materialización del incidente tiene medianos efectos dentro de los procesos de la PGN.	40% A 60%
2	Mínimo	La materialización del incidente tiene efectos mínimos dentro de los procesos de la PGN.	20% A 40%
1	Insignificante	La materialización del incidente tiene efectos no significativos dentro de los procesos de la PGN	0 A 20%

TRATAMIENTO DEL REGISTRO DEL INCIDENTE

Para disponer de toda la información acerca del incidente se registrará como mínimo en la base de gestión de conocimiento la información concerniente a:

- fecha y hora de aparición del incidente
- tipología y gravedad del mismo
- recursos afectados
- posibles orígenes
- estado actual del incidente
- acciones realizadas para solventarlo y quienes las ejecutaron
- fecha y hora de resolución y cierre del incidente
- impacto generado

LECCIONES APRENDIDAS

El objetivo es que las lecciones de los incidentes de seguridad de la información, vulnerabilidades y gestión asociada se aprendan rápidamente, se documenten en una base de gestión de conocimiento (Knowledge Database), para evitar la posible ocurrencia de futuros incidentes de seguridad de la información, mejorar la implementación y uso de controles de seguridad de la información y fortalecer el esquema general de gestión de incidentes de seguridad de la información.

6.14. POLÍTICA DE GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación la política de gestión y clasificación de activos de información.

POLITICA

Esta política establece los criterios con los cuales la PGN identifica los activos de información y asigna valor a los mismos; de igual forma, proporciona a los funcionarios indicaciones sobre el uso apropiado de los activos de información con el propósito de proteger a la Entidad y sus activos de información.

RESPONSABILIDADES

GESTIÓN DE ACTIVOS

La oficina de Sistemas de la PGN en conjunto con los responsables de los procesos se comprometen a identificar, clasificar, etiquetar, disponer, valorar y gestionar los activos de información de acuerdo al Instructivo para el proceso de inventario y clasificación de activos de información y normas aplicables para la clasificación de activos de información.

Para el etiquetado de la información se debe tener en cuenta la Guía de clasificación de información, de igual manera el Instructivo para la identificación y clasificación de activos de información.

El uso de dispositivos móviles que almacenen información de la PGN y que a su vez se utilicen para el manejo de esta información, deben ser controlados de acuerdo a la *Política de Dispositivos Móviles*, para el tratamiento y mitigación del impacto al cual se expone la información como su pérdida, alteración y divulgación no autorizada, por lo cual la PGN debe contar con un inventario actualizado de los dispositivos utilizados para los fines ya mencionados, teniendo en cuenta que deben cumplir con unos requisitos establecidos para la protección de la información y restricción de conexión a servicios en los que exista información de la Entidad.

En el caso que el dispositivo móvil tenga fines de traslado de información debe cumplir con la *Política de Dispositivos Móviles* y la *Política sobre el uso de controles criptográficos*; si el uso del dispositivo es temporal se debe tener en cuenta el procedimiento de intercambio seguro de información, adicionalmente contar con una copia de respaldo de la información de acuerdo con lo establecido en la *Política de Copias de Seguridad*, teniendo en cuenta la clasificación de la información que se encuentre almacenada. Para el respaldo de la información es necesario tener en cuenta los lineamientos establecidos en el Procedimiento de Copias de Seguridad, además se deben generar recomendaciones sobre el uso y cuidado de tipo físico cuando el dispositivo se encuentre fuera de las instalaciones de la Entidad.

Se debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, con el fin de gestionar los activos desde su adquisición hasta su eliminación con el fin de asegurar que se utilizan eficaz y eficientemente y sean contabilizados y protegidos físicamente.

Los activos de información deben tener un uso aceptable siguiendo las siguientes indicaciones definidas, así:

Protección de la confidencialidad, disponibilidad e integridad:

De acuerdo con la clasificación del activo frente a la confidencialidad, disponibilidad e integridad, el funcionario que está accediendo a la información debe verificar que cuenta con los permisos para hacerlo de acuerdo con su rol; en caso contrario debe abstenerse de hacerlo e informar del hecho a su Jefe Inmediato y al oficial de Seguridad de la Información o quien haga sus veces en la oficina de sistemas, para que se tomen las medidas pertinentes.

Los funcionarios, proveedores y/o terceros de la Procuraduría General de la Nación que accedan, modifiquen o hagan uso de la información, únicamente pueden compartir aquella información con los funcionarios que tengan autorización para ello, de acuerdo con lo estipulado en la Política de relación con proveedores.

Todos los funcionarios, proveedores y/o terceros de la Procuraduría General de la Nación están obligados a reportar accesos o modificaciones no autorizados o uso indebido de un activo.

Uso de la Información digital y física:

Los responsables de los activos de información deben asegurar que el acceso a éstos se realice dependiendo su nivel de clasificación, basado en la valoración dada al activo.

Los responsables de los activos de información deben asegurar que éstos se encuentren actualizados cuando se produzca un cambio en su medio de almacenamiento, ubicación, responsable y custodio.

Recursos Compartidos:

El funcionario que autoriza y dispone un recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicho recurso.

Para el acceso y los permisos de: lectura, ejecución, escritura, modificación y borrado de la información sobre las carpetas compartidas se debe dar cumplimiento a los lineamientos establecidos en la Política de control de acceso.

Si se trata de información reservada o restringida para la PGN, deben utilizarse las carpetas de red destinadas para tal fin en el espacio de almacenamiento que la Oficina de Sistemas disponga para este fin, con el fin que se realicen y automaticen las respectivas copias diarias de respaldo de la información.

El acceso a carpetas compartidas deben ser autorizadas por la Oficina de Sistemas, delimitadas a los funcionarios y deben estar protegidas con contraseñas.

Licenciamiento:

Es responsabilidad de la Oficina de Sistemas la administración e instalación de las licencias necesarias del software adquirido por la Entidad de acuerdo a su necesidad.

CLASIFICACIÓN DE LA INFORMACIÓN.

La PGN cuenta con un sistema de Gestión documental establecido en la Caracterización del subproceso de administración de documentos y registros *CAR-PRO-GR-002*.

Para la clasificación de su información la Entidad adopta la siguiente normatividad:

- Resolución No 669 del 13 de diciembre de 2017 Por medio de la cual se adoptan los Instrumentos de Gestión de la Información Pública.
- Resolución 670 del 14 de diciembre 2017 Por medio de la cual se adopta el Manual de Políticas y Procedimientos para la protección de datos personales.
- Comunicación 2501 del 06 de diciembre de 2017 por medio de la cual el Jefe de la Oficina Jurídica da visto bueno a la matriz índice de información clasificada y reservada.
- Índice de tablas de retención documental de la PGN.

- Guía 5 para la Gestión y Clasificación de Activos, Estrategia Gobierno Digital MINTIC, capítulo 7.

La PGN de acuerdo a la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, Ley 1712 de 2014 según el artículo No. 6, clasifica su información de acuerdo con la siguiente tabla:

Tipos de clasificación	Descripción
Información Pública	Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
Información Pública Clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en al artículo 18 de esta ley.
Información Pública Reservada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de totalidad por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Fuente: Guía 5 para la Gestión y Clasificación de Activos, Estrategia Gobierno en Línea (GEL) MINTIC, capítulo 7.

La anterior información puede ser consultada en el link:

https://www.procuraduria.gov.co/portal/transparencia.page - Numeral 10.Instrumentos de Gestión de Información Pública

Con el fin de brindar continuidad al proceso y mantener la actualización necesaria según la legislación vigente, la Entidad realizará revisiones periódicas a la clasificación de la información.

ETIQUETADO Y MANEJO DE LA INFORMACIÓN.

Para el manejo de la información, se debe tener en cuenta que en caso que la información se encuentre en uso por personal autorizado y se encuentre

clasificada como Información Pública, Información Pública Clasificada o Información Pública Reservada los funcionarios responsables deben velar por la adecuada protección de la misma, con el fin de evitar la divulgación o reproducción no autorizada a otras personas.

Para la protección adecuada, se recomienda no dejar desatendida la información en ningún momento de tiempo, según lo preceptuado en la *Política de escritorio y pantalla limpia* de la PGN. En caso que dicha información no se encuentre en uso, es recomendable que ésta permanezca centralizada con la seguridad física y/o lógica pertinente (bajo llave, en archivadores o en cajas fuertes si llegase a ser necesario) y los propietarios deben velar por salvaguardar de forma adecuada la misma.

COMPROMISO CON EL MEJORAMIENTO CONTINUO

Si los funcionarios, contratistas y/o terceros de la Procuraduría General de la Nación se dan cuenta de incumplimientos en el uso de algún activo de información por parte de alguno de los actores que hace parte del SGSI, deben informarlo de manera oportuna a la Oficina de Sistemas o a los propietarios de los activos de información y en el caso de contratistas, al supervisor del contrato, para que se tomen las medidas pertinentes.

6.15. POLÍTICA DE RELACIÓN CON PROVEEDORES

OBJETIVO

Establecer por parte de la Procuraduría General de la Nación los lineamientos de seguridad de la información para terceros, contratistas y proveedores con el fin de mantener los principios de: confidencialidad, disponibilidad e integridad de la información de la Entidad.

POLITICA

La Procuraduría General de la Nación necesita contratar servicios especializados externos que den soporte a parte de su actividad. En estos casos se debe exigir a los proveedores externos la misma seguridad interna para que puedan gestionar parte de la información de la Entidad (sobre todo si es información sensible). Entre estos proveedores se pueden definir los siguientes grupos:

Proveedores de servicios tecnológicos. Aquellos que ofrecen servicios como alojamiento web, suministro del canal de internet, emisión de certificados, servicio de portales de pago, servicios de almacenamiento en la nube, servicios de soporte informático (tanto presencial como remoto), productos y servicios instalados en prueba concepto, etc.

Proveedores de servicios no tecnológicos, pero que acceden a datos corporativos. Tales como proveedores de servicios financieros, viajes, transporte, publicidad, marketing, etc.

Proveedores que suministran productos tecnológicos. Incluyen todos aquellos dónde se adquieren los equipos, dispositivos, appliances, componentes hardware y las aplicaciones informáticas.

Esta política está enfocada en controlar que toda relación con proveedores, y en particular aquellos que tienen acceso a la información de la PGN, está protegida con base en los acuerdos y contratos correspondientes, antes, durante y a la finalización del contrato o servicio prestado. También es deber asegurar que los productos y servicios contratados cumplen con los requisitos de seguridad informática establecidos por la Entidad.

RESPONSABILIDADES

Para la mitigación de los posibles riesgos asociados con el acceso de proveedores y contratistas a los activos de información de la Entidad, se establecen los siguientes lineamientos de Seguridad de la información entre la PGN y sus proveedores y/o contratistas:

- Los proveedores y/o contratistas que tengan acceso a los activos de información están obligados a cumplir las Políticas de Seguridad de la Información definidas y reportar los incidentes de seguridad de la información a la Oficina de Sistemas de la Entidad.
- Los proveedores y/o contratistas no podrán tener acceso a áreas o zonas donde se encuentre información sensible en la Entidad. Si fuese necesario su ingreso a determinadas áreas, será necesaria la autorización de un funcionario de la Entidad, el cual debe acompañar al contratista durante el tiempo que este permanezca en dicha área.

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN CON PROVEEDORES

- Para el intercambio de información entre la PGN sus proveedores y/o contratistas, se deberán implementar estándares y procedimientos formales asociados al intercambio de información, que permitan garantizar la seguridad en el acceso y la transferencia de información, de acuerdo con lo referido en la *Política de transferencia de información* de la Entidad.
- Los proveedores y/o contratistas que tengan relaciones contractuales con la Entidad, deben incluir dentro de su contrato cláusulas de Confidencialidad de la información.
- La contratación de los proveedores y/o contratistas se realiza de acuerdo a lo establecido en el Manual de Contratación de la Entidad *MAN-CN-00-001*.

TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON LOS PROVEEDORES

- Los controles fisicos y lógicos con los cuales el proveedor y/o contratista que tenga relación contractual con la PGN deben cumplir deberán estar documentados y aprobados por la Oficina Asesora Jurídica y ser de conocimiento de ambas partes.
- Los funcionarios responsables de la PGN deberán establecer una lista detallada del personal autorizado por el proveedor, especificando quienes puedan tener acceso a la información de la Entidad o recibirla de ella.
- Para la modificación y/o adquisición de software el proveedor deberá realizar pruebas con el solicitante del nuevo desarrollo o cambio en alguna aplicación existente con el fin de validar la funcionalidad y disponibilidad de la aplicación. Adicionalmente el desarrollador deberá entregar un manual de usuario con las especificaciones técnicas y funcionales de la aplicación.
- Los proveedores notificarán a la Oficina de Sistemas, sobre los incidentes de seguridad de la información que hayan sucedido o materializado en el marco del servicio prestado; así mismo, se documentará la gestión y acciones tomadas para el cierre del incidente.
- La PGN mantendrá actualizada la información correspondiente de la persona de contacto que los proveedores tenga asignada con respecto a la seguridad de la información.
- Se debe determinar qué información es accedida, cómo puede ser accedida y la clasificación y protección de la misma.
- Asegurar de que una vez finalizado el contrato, el proveedor ya no podrá acceder o mantener la información sensible de la PGN
- Se debe establecer el cumplimento de los derechos de propiedad intelectual.
- Todo contrato debe definir las garantías especificas, que contemplen penalizaciones económicas en caso de incumplimiento, perjuicios económicos por inactividad, y certificaciones y garantías adicionales.

CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

- Para toda adquisición de software y hardware realizada por la PGN, La Oficina de Sistemas, será la responsable de definir los requisitos de seguridad, los cuales deben quedar documentados y aprobados por las partes en el contrato u acuerdo.
- Los proveedores y contratistas que acuerdan externamente servicios de otras compañías, y que estén relacionados con el suministro de tecnologia de información y comunicación que prestan a la PGN, deberán proporcionar información sobre los requisitos y prácticas de seguridad, a quienes se les realizará el respectivo seguimiento por parte de la PGN, según los acuerdos iniciales establecidos con el proveedor del servicio.

SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES

Es importante asegurar que los términos y condiciones de seguridad de la información en los acuerdos realizados entre la PGN con los proveedores y/o contratistas se cumplan, así como los incidentes que se generen sean gestionados oportunamente, para lo cual:

- Se realizará seguimiento y revisión a los productos y servicios prestados por los proveedores de acuerdo a las condiciones iniciales establecidas dentro del contrato.
- De acuerdo al proveedor o contratista, se definirá los mecanismos que permitan realizar el seguimiento, dependiendo de la criticidad de la información que maneja, evaluando criterios de seguridad física y lógica, así como algunos requerimientos del estándar ISO/IEC 27001- 2013.
- De ser posible y si aplica, para proveedores de alto impacto en seguridad de la información se evalúa el plan de continuidad del proveedor.
- El seguimiento o auditoria a los procesos y controles a los proveedores se realizará con una periodicidad no mayor a un año.
- La Oficina de Sistemas tendrá la responsabilidad de verificar y validar la configuración de los equipos instalados, de igual manera reportar las debilidades y oportunidades de mejora al proveedor del servicio a través de los procedimientos internos establecidos por la Entidad.
- Los proveedores que entreguen servicios a la Entidad deben contar con certificaciones vigentes de seguridad de la información y/o firmas digitales, aplicado a los servicios que se contratarán en especial en los casos en que se externalice los procesos de tratamiento y resguardo de información, ya sean hosting, housing, entre otros.
- Para los proveedores que tengan relación con almacenamiento, comunicación, infraestructura, plataforma o software que sean entregados a la Entidad en modalidad de servicio, como servicios en la nube, equipos tecnológicos adquiridos o sistemas de información desarrollados por terceros y sobre los cuales existan garantías del fabricante, se deben establecer y documentar procedimientos para la gestión de incidentes de seguridad, los que serán gestionados a través de la mesa de servicios bajo los procedimientos internos ya definidos.
- Es necesario establecer acuerdos de niveles de servicio (ANS) los cuales deben ser formalizados a través de bases de licitación, actos administrativos o acuerdos complementarios que contengan criterios relacionados con el nivel de servicio, entrega continua del mismo, tiempos de respuesta de atención para su entrega, tiempos de resolución de problemas, entre otros, que serán aplicados por el área respectiva que solicita el servicio y asesorados por la Oficina de Sistemas.
- Para el monitoreo sobre los servicios tecnológicos tercerizados será responsabilidad de la Oficina de Sistemas incorporar un control de monitoreo asegurando la disponibilidad de los servicios tecnológicos,

plataformas de infraestructura y los sistemas de información que sean entregados por el proveedor, con el propósito de medir los niveles del servicio y gestionar de manera oportuna cualquier incidente que puedan afectar el principio de disponibilidad.

GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES

Cuando se presenten cambios en los Acuerdos con los proveedores, tanto el proveedor o contratista como la PGN deben establecer y notificar las modificaciones que se generen o se estimen realizar con respecto a los acuerdos contractuales iniciales.

Con respecto a los cambios que la PGN requiera implementar como mejoras al servicio ofrecido, desarrollo de nuevas aplicaciones y sistemas, actualizaciones o modificaciones a las Políticas de Seguridad de la Entidad, estará en función del *Comité de Seguridad de la Información* la definición de los lineamientos de seguridad que se deben aplicar para cumplir con los requisitos del Sistema de Gestión de Seguridad de la Información.

Todo cambio en el servicio que el proveedor o contratista desee o requiera implementar que involucre el uso de nuevas tecnologías, cambios y mejoras en las redes, actualización de versiones o ediciones recientes, herramientas nuevas y ambientes de desarrollo, deben ser informados a la PGN antes de ser implementados.

6.16. POLÍTICA DE REQUERIMIENTOS LEGALES, REGULATORIOS Y CONTRACTUALES

OBJETIVO

Identificar, documentar y mantener actualizados por parte de la Procuraduría General de la Nación los requerimientos legales, regulatorios y contractuales relativos a Seguridad de la Información.

POLITICA

La Procuraduría General de la Nación garantiza el cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

RESPONSABILIDADES

La Oficina Asesora Jurídica de la PGN deberá identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Entidad y en particular aquellos relacionados con la Seguridad de la Información.

La Oficina de Sistemas es responsable de la verificación del software que se ejecuta en la PGN, debe velar por la protección de derechos de autor y que su uso se encuentre debidamente autorizado (licenciamiento).

La Oficina de Sistemas debe mantener actualizado el inventario de hardware, software y sistemas de información que se encuentran instalados en los equipos de la PGN, además debe verificar que el software instalado corresponda al autorizado.

En cumplimiento de la Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la PGN propenderá por la protección de los datos personales de los terceros de los cuales reciba y administre información.

Si los funcionarios, contratistas y/o proveedores de la PGN se dan cuenta de un incumplimiento en cuanto a la normatividad aplicable a la PGN, deben informar a la Oficina de Sistemas para que se tomen las medidas pertinentes.

SANCIONES

Los funcionarios, contratistas y/o terceros de la PGN tienen la responsabilidad de adherirse a esta política de requerimientos legales, regulatorios y contractuales. Cualquier incumplimiento de esta política en caso de que se determine no seguir los lineamientos establecidos para cumplimiento de leyes y normatividad, y que ponga en riesgo algún aspecto del SGSI, puede constituir una falta y se aplicarán las sanciones pertinentes.

NORMATIVIDAD APLICABLE

A continuación se relaciona los requerimientos legales, regulatorios y contractuales vigentes y aplicables para la Entidad en relación con la Seguridad de la Información.

Tipo	Número	Año	Descripción
Ley	57	1985	Por la cual se ordena la publicidad de los actos y documentos oficiales
Ley	527	1999	Por medio de la cual se define y reglamenta el comercio electrónico.
Ley	594	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley	1266	2008	Disposiciones generales de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

Tipo	Número	Año	Descripción
Ley	1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley	1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley	1581	2012	Por el cual se dictan disposiciones generales para la protección de Datos Personales.
Ley	1712	2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto	1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Reglamentación parcial de la Ley de Protección de Datos Personales.
Decreto	1524	2002	Por el cual se reglamenta el artículo 5 de la Ley 679 de 2001, Establece las medidas técnicas y administrativas destinadas a prevenir el acceso a menores de edad a cualquier modalidad de información pornográfica contenida en internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.
Decreto	2693	2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones
Decreto	2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto Reglamentario Único	1081	2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República
Acuerdo	03	2015	Archivo General de la Nación Por el cual se establecen lineamientos generales para las Entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos
Decreto	2364	2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones

Tipo	Número	Año	Descripción
Decreto	1747	2000	Entidades de certificación, los certificados y las firmas digitales
Decreto	1078	2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto	262	2000	(Capitulo Primero) asigna al grupo de Infraestructura la seguridad Informática de la Entidad, este grupo constituye e integra el Comité de Seguridad de la Información de la Entidad.
Decreto	1008	2018	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto	1413	2017	"Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Norma Técnica Colombiana NTC	5854	2011	Accesibilidad a páginas web
Norma Técnica Colombiana NTC-ISO-IEC	27001	2013	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la Información. Requisitos
Guía Técnica Colombiana GTC-ISO-IEC	27035	2013	Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información
Guía MINTIC	V3	2016	Datos abiertos en Colombia
Guía MINTIC	V1	2016	Innovación abierta por medios electrónicos
Guía MINTIC	V1	2016	Gobierno en redes
Guía MINTIC	V1	2016	Atención al ciudadano/cliente por múltiples canales

Tipo	Número	Año	Descripción
Guia MINTIC	V1	2016	Diseño de un Plan Estratégico de las Tecnologías de Información
Guia MINTIC	V1	2016	General de Adopción del Marco de Referencia de Arquitectura Empresarial
Guia MINTIC	V1	2016	Indicadores del dominio de Estrategia del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado
Guia MINTIC	V1	2016	Para la definición del portafolio de servicios de TI del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI
Guia MINTIC	V1	2014	Técnica Básica de Información del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI
Guia MINTIC	V1	2016	Dominio de Sistemas de Información del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI
Guia MINTIC	V1	2016	Técnica de Sistemas de Información - Trazabilidad del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI.
Guia MINTIC	V1	2016	Dominio de Servicios Tecnológicos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI
Guia MINTIC	V1	2016	Dominio de Uso y Apropiación del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI
Guia MINTIC	V1	2016	Roles y Responsabilidad de Seguridad de la Información
Guia MINTIC	5	2016	Gestión De Activos
Guia MINTIC	8	2016	Controles de Seguridad
Guia MINTIC	14	2016	Plan de comunicación, sensibilización y capacitación:
Guia MINTIC	15	2016	Auditoria
Guia MINTIC	16	2016	Evaluación del desempeño
Guia MINTIC	17	2016	Mejora Continua
Guia ICC		2016	INFRAESTRUCTURA CRÍTICA CIBERNÉTICA
Manual	V1	2017	Estrategia de Gobierno en línea
Manual	V1	2018	DAFP, Manual Operativo Sistema de Gestión MIPG 3.2.1.4 Política de Seguridad Digital
Resolución PGN	010	2017	Por medio de la cual se adopta el Programa de Gestión Documental de la Procuraduría General de la Nación y se modifica la Resolución 231 de 2007.
Resolución PGN	011	2017	Por la cual se adopta el teletrabajo en la Procuraduría General de la Nación.

Tipo	Número	Año	Descripción
Resolución PGN	291	2018	Por medio de la cual se crea el Grupo de informática Forense en la Dirección Nacional de Investigaciones Especiales.
Resolución PGN	302	2005	Por medio de la cual se determinan las políticas de uso de los equipos de cómputo de la Procuraduría General de la Nación y los servicios institucionales de Correo Electrónico e Internet, el manejo, instalación y desinstalación de software y la conservación y cuidado de la información afectada al funcionamiento de la Entidad.
Resolución PGN	342	2004	Por medio de la cual se reglamenta la prestación del servicio de los auxiliares jurídicos ad-honorem creados por la Ley 878 de enero de 2004
Resolución PGN	370	2015	Por la cual se adopta el Manual de Contratación de la Procuraduría General de la Nación y se efectúan algunas modificaciones a otras disposiciones.
Resolución PGN	670	2017	Por medio de la cual se adopta el manual de políticas y procedimientos para la protección de los datos personales
Resolución MINTIC	3564	2015	Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública

Fuentes: Min TIC – PGN – Diario Oficial – ISO

6.17. POLÍTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

OBJETIVO

Definir por parte de la Procuraduría General de la Nación - PGN, los lineamientos para la privacidad y protección de información de datos personales, garantizando la confidencialidad, autenticidad e integridad de la información de la entidad de acuerdo a lo establecido en la Ley 1581 de 2012.

POLITICA

La Procuraduría General de la Nación mediante la Resolución 670 del 14 de diciembre del 2017 adopta el manual de Políticas y Procedimientos para la Protección de Datos Personales, documento que establece la forma como se recopilan, manejan y conservan los datos personales de los sujetos que la entidad en desarrollo de sus funciones constitucionales y legales requiere de su uso; y señala el procedimiento por el cual el interesado puede acudir ante la administración para solicitar el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de sus datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales que allí mismo se señalan.

7. FASES DE IMPLEMENTACIÓN

Para realizar una correcta implementación de las políticas específicas anteriormente mencionadas se debe tener en cuenta las siguientes fases de implementación:

7.1. Desarrollo.

En esta fase la PGN establecerá las políticas específicas de Seguridad de la Información, las cuales deben ser revisadas y aprobadas por la alta Dirección; una vez publicadas serán de obligatorio cumplimiento para los funcionarios, contratistas y/o terceros con acceso a la información. Los responsables del SGSI deben velar por el cumplimiento, la revisión y actualización de estas políticas.

7.2. Cumplimiento.

En esta fase la PGN debe comprometerse a destinar los recursos necesarios para la implementación, mantenimiento y cumplimiento de las políticas específicas de Seguridad.

7.3. Comunicación.

En esta fase la PGN dará a conocer a todos los funcionarios, contratistas y/o terceros de las políticas especificas de Seguridad de la Información, así como, la obligatoriedad de su cumplimiento y la ubicación física del documento que las contiene, para que sean consultados en el momento que se requiera.

7.4. Monitoreo.

En esta fase la PGN debe establecer los mecanismos de monitoreo (p. e. indicadores, métricas, auditorías internas y externas) que permitan medir y determinar la efectividad y cumplimiento de las políticas especificas de Seguridad de la Información.

7.5. Mantenimiento.

En esta fase la PGN debe asegurar que las políticas especificas de Seguridad de la Información se encuentren actualizadas, integras y que sean ajustadas con base en los resultados de la fase de monitoreo.

7.6. Retiro.

En esta fase la PGN definirá los mecanismos de eliminación de las políticas específicas de Seguridad de la Información en cuanto estas hayan cumplido su finalidad o ya no sean necesarias en la Entidad. En esta última fase y para dar

cumplimiento al ciclo de vida de las políticas de Seguridad de la Información se requiere que este retiro sea documentado con el objetivo de tener referencias y antecedentes sobre el tema.

8. NIVEL DE CUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad de la Información es de carácter obligatorio, cada uno de los funcionarios, contratistas y/o terceros debe comprender su rol y asumir su responsabilidad respecto a los riesgos en Seguridad de la Información y la protección de los activos de información de la Entidad.

El incumplimiento de las políticas de Seguridad de la Información que comprometa la confidencialidad, disponibilidad e integridad de la información puede resultar en una acción disciplinaria o en acciones legales que apliquen a la normatividad del Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información.

Las políticas de seguridad de información de la Procuraduría General de la Nación están desarrolladas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en la normatividad vigente. Si algún funcionario, contratista y/o tercero de la Entidad considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al personal encargado de la seguridad informática de la Entidad.

9. ADMINISTRACIÓN DE LAS POLÍTICAS

Las Políticas de Seguridad de la Información se deben preservar en el tiempo y están sujetas a una revisión anual o en el evento de cambios estructurales que afecten a la Procuraduría General de la Nación, para asegurar que éstas se ajusten a las necesidades de la Entidad.

La fecha de vigencia de las Políticas de Seguridad de la Información será a partir de su aprobación por parte de la Alta Dirección.

El Oficial de Seguridad de la Información o el funcionario designado por la alta Dirección será el responsable de brindar información acerca de las políticas de Seguridad de la Información.

Ante la necesidad de un cambio en las políticas de Seguridad de la Información y con el fin de contribuir a un mejoramiento continuo de las mismas, se deben comunicar los cambios realizados a todos los usuarios internos, externos, terceros y a quienes de manera directa o indirecta apliquen.

PROCURADURIA
GENERAL DE LA NACION

10. DEFINICIONES

Las expresiones utilizadas en este documento deben ser entendidas con el significado que a continuación se indica. Los términos definidos son aplicados en singular y en plural de acuerdo como lo requiera el contexto en el cual son considerados. Y aquellos que no se encuentren definidos a continuación, deben entenderse con su significado natural.

Activo de Información	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.[1]
Acuerdos de Niveles de Servicio (SLA)	"Service Level Agreement" o "Acuerdo de Nivel de Servicio". Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.[2]
Administración del Riesgo	Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.[3]
Ambiente (de desarrollo, pruebas o producción)	Es la infraestructura tecnológica (hardware y software) que permite desarrollar, probar o ejecutar todos los elementos o componentes para ofrecer un servicio de Tecnologías de la Información.[4]
Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.[5]
Amenaza informática	Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.[6]
Análisis de riesgo	Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.[7]
Antivirus	Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El

[1] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf el 08/05/2019 a las 9:45 am
[2] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf el 08/05/2019 a las 9:30 am
[3] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 09/05/2019 a las 4:20 pm
[4] Consulta realizada en https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html el 08/05/2019 a las 10:50 am
[5] NTC ISO/IEC 27000:2013
[6] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 10:55 am
[7] NTC ISO/IEC 27000:2013

	antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.[8]
Archivo	Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.[9]
Aplicaciones engañosas	Son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.[10]
Archivos de Log	Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.[11]
Autenticación	Provisión de una garantía de que una característica afirmada por una entidad es correcta.[12]
Autenticidad	Propiedad de que una entidad es lo que afirma ser.[13]
Autorización	Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.[14]
Aviso de privacidad	Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.[15]
Bases de Datos Personales	Conjunto organizado de datos personales que sea objeto de Tratamiento[16]

[8] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 10:55 am
[9] Ley 1712 de 2014, art 6
[10] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 10:55 am
[11] CONPES 3701 - LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. Pag 19
[12] NTC ISO/IEC 27000:2013
[13] NTC ISO/IEC 27000:2013
[14] Ley 1581de 2012, art 3
[15] Decreto 1377 de 2013, art 3
[16] Ley 1581 de 2012, art 3

Base de conocimiento	Portafolio de instrumentos y herramientas que guían y ayudan a la implementación del Marco de Referencia de Arquitectura Empresarial para la gestión de Tecnologías de Información.[17]
Centro de procesamiento de datos	Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.[18]
Certificado de servidor seguro	Son Certificados en software que identifican que una determinada página web pertenece a una determinada empresa y que la información transmitida entre el usuario de la página y el servidor está cifrada, de forma que no pueda ser vista ni manipulada por terceros.[19]
Certificado de firma Digital	Es un documento electrónico que se emite a una persona o entidad, contiene datos que acreditan la identidad del titular del certificado ante terceros, tiene asociado un par de llaves (llave pública y llave privada), posee un periodo de vigencia implícito, es emitido y firmado por una Autoridad Certificadora reconocida como tal que garantiza que el titular del certificado es quien dice ser.[20]
Ciberespacio	Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.[21]
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[22]
Cifrado	Mecanismo por el cual se emplean algoritmos matemáticos y un sistema de claves que sólo son identificados entre la persona que navega y el servidor.[23]
Clasificación de la información	Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado[24]

[17] Consulta realizada en https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8158_descargable_6.pdf el 08/05/2019 a las 4:05 pm

[18] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf el 08/05/2019 a las 9:30 am

[19] Consulta realizada en https://www.camerfirma.com/ayuda/faq/certificados-de-servidor-seguro/ el 08/05/2019 a las 4:15 pm

[20] Consulta realizada en https://www.andescd.com.co/index.php?option=com_content&view=article&id=4&Itemid=114 el 08/05/2019 a las 4:15 pm

[21] Resolución CRC 2258 de 2009

[22] CONPES 3701

[23] Extraido de https://www.certsuperior.com/QueesunCertificadoSSL.aspx el 18/05/2019 a las 4:25 pm

[24] Tomado de NTC ISO/IEC 27000:2013

Confidencialidad	Propiedad de la información que determina que esté disponible a personas autorizadas. [25]
Contraseña	Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña. [26]
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.[27]
Correo Electrónico Certificado	Plataforma de Correo Electrónico que proporciona un servicio de notificación electrónica por e-mail que cuenta con la misma validez jurídica y probatoria de un envío certificado por medios físicos y con mayores fortalezas funcionales, técnicas y jurídicas que el email electrónico convencional o no certificado.[28]
Correo Electrónico Institucional	Es el servicio de correo electrónico que provee y administra directamente la Procuraduría General de la Nación a sus funcionarios, como herramienta de apoyo a las funciones y responsabilidades de los mismos.[29]
Custodio de activo de información	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. [30]
Data Center	Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.[31]
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;[32]

[25] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 4:30 pm

[26] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf el 09/05/2019 a las 3:00 pm

[27] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf el 08/05/2019 a las 9:30 am

[28] Tomado de https://web.certicamara.com/productos_y_servicios/Plataformas_Cero_Papel/42-Correo_Electr%C3%B3nico_Certificado_-_Certimail el 08/05/2019 a las 4:40 pm

[29] Resolución 302 de 2005 – PGN, art 1

[30] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf el 08/05/2019 a las 4:44 pm

[31] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf el 08/05/2019 a las 9:30 am

[32] Ley 1581de 2012, art 3

Dato público	Es el dato que no sea serniprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.[33]
Dato semiprivado	Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.[34]
Datos Abiertos	Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos[35]
Datos sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello 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.[36]
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera[37]
Dispositivo Móvil	Un dispositivo móvil se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales.[38]

[33] Decreto 1377 de 2013, art 3
[34] Ley 1581 de 2012, art 2.5.6.2
[35] Ley 1712 de 2014, art 6
[36] Decreto 1377 de 2013, art 3
[37] NTC ISO/IEC 27000:2013
[38] Consulta realizada en https://sites.google.com/site/dispositivosmovilesyulianah/concepto-general-dispositvo-movil el 08/05/2018 a las 4:55 pm

Documento de archivo	Es el registro de información producida o recibida por una Entidad de archivo pública o privada en razón de sus actividades o funciones.[39]
Encargado del Tratamiento	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento[40]
Encriptación	La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.[41]
Estampado cronológico	Corresponde al suministro de marcas de tiempo para asociar a los documentos electrónicos una referencia temporal que garantice técnicamente que la serie de datos presentada por el solicitante ha existido y no ha sido modificada desde un momento cierto lo cual permite que la fecha y hora obtenidos en la marca en virtud de ser impuestas por sistema independiente y ajeno al procedimiento confiera garantía de imparcialidad ante un posible litigio.[42]
Evaluación del Riesgo	Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.[43]
Evento de seguridad de la información	Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.[44]
Exploits o Programas intrusos	Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.[45]
Firma digital	Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el

[39] Ley 1712 de 2014, art 6
[40] Ley 1581 de 2012, art 3
[41] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf el 09/05/2019 a las 3:00 pm
[42] Consulta realizada en https://www.andesscd.com.co/index.php?option=com_content&view=article&id=6&Itemid=116 el 08/05/2019 a las 3:39 pm
[43] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 09/05/2019 a las 4:20 pm
[44] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 08/05/2019 a las 5:00 pm
[45] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:39 pm

	mensaje inicial no ha sido modificado después de efectuada la transformación;[46]
Gestión de incidentes de seguridad de la información	Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.[47]
Gestión documental	Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.[48]
Incidente de seguridad de la información	Uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.[49]
Información	Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.[50]
Información pública	Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal[51]
Información pública clasificada	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014[52]
Información pública reservada	Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley[53]
Integridad	La propiedad de salvaguardar la exactitud y complejidad de los recursos[54]
Inventario de activos	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.[55]

[46] Ley 527 de 1999, art 2
[47] ISO/IEC 27000
[48] Ley 1712 de 2014, art 6
[49] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 18/05/2019 a las 5:00 pm
[50] Ley 1712 de 2014, art 6
[51] Ley 1712 de 2014
[52] Ley 1712 de 2014
[53] Ley 1712 de 2014
[54] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 18/05/2019 a las 5:00 pm
[55] ISO/IEC 27000

Malware	El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse.[56]
NAS	Por sus siglas en inglés Network Attached Store, se refiere a Almacenamiento en red.
No repudio	Es el atributo que brinda protección contra la denegación por parte de una de las partes que interviene en un trámite ante el estado a través del servicio ciudadano digital de interoperabilidad.[57]
Parte interesada (Stakeholder)	Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad[58]
Phishing	Método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.[59]
Proceso	Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.[60]
Propietario de activo de información	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.[61]
Proveedor de redes y servicios	Persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros.[62]
Publicar o divulgar	Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.[63]

[56] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf el 09/05/2019 a las 3:10 pm
[57] Consulta realizada en http://micrositios.mintic.gov.co/servicios_ciudadanos_digitales/autenticacion_electronica/3_1_manual_condiciones_servicio_autenticacion_electronica.pdf el 09/05/2019 a las 4:10 pm
[58] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf el 08/05/2019 a las 10:00 am
[59] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:55 pm
[60] ISO/IEC 27000
[61] Consulta realizada en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf el 08/05/2019 a las 4:05 pm
[62] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:58 pm
[63] Ley 1712 de 2014, art 6

Red de servicios	Es aquella conformada por los nodos de servicio y por enlaces que interconectan los nodos entre si.[64]
Responsable del tratamiento	Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.[65]
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.[66]
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información[67]
Sistema de Gestión de Seguridad de la Información SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua[68]
Smishing	Es una variante del phising, pero a diferencia de este, usa mensajes de texto para engañar a los usuarios, pidiéndoles información privada e invitándolos a que se dirijan a sitios web falsos que tienen spywares y softwares maliciosos que se descargan automáticamente, sin que el usuario lo note.[69]
Software CommVault	Es un software para la administración de datos e información, a través del cual se hace la administración total del ciclo de vida de los datos criticos de la Entidad. Se ejecuta sobre plataforma Windows.[70]
Spam	También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.[71]
Spyware o Programa espia	El software espia consta de un paquete de software que realiza un seguimiento y envia información confidencial o personal a

[64] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 4:00 pm
[65] Ley 1581 de 2012, art 3
[66] ISO/IEC 27000
[67] ISO/IEC 27000
[68] Ibidem
[69] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:30 pm
[70] Fuente: Administrador copias de respaldo PGN
[71] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:30 pm

	terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.[72]
Streaming	Consiste en una tecnología utilizada para permitir la visualización y la audición de un archivo mientras se está descargando, a través de la construcción de un buffer por parte del cliente, una vez que éste se ha conectado al servidor, el buffer del cliente se va llenando de la información descargada y se va reproduciendo en el ordenador. El sistema se encuentra sincronizado, tal que, una vez terminada la reproducción del contenido del archivo, finaliza la descarga (siempre y cuando no existan interrupciones en el envío del archivo).[73]
Sujetos obligados	Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5 de la Ley 1712 de 2014.[74]
Teletrabajo	Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.[75]
Teletrabajador	Persona que desempeña actividades laborales a través de tecnologías de la información y la comunicación por fuera de la empresa a la que presta sus servicios.[76]
Titular de la información	Personas naturales cuyos datos personales sean objeto de Tratamiento.[77]
Token	En sistemas de seguridad, pequeño dispositivo del tamaño de una tarjeta de crédito que muestra un código de ID que constantemente cambia. Primero un usuario ingresa una clave y luego la tarjeta muestra un ID que puede ser usado para ingresar a una red.[78]
Transferencia de datos	La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.[79]

[72] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:30 pm
[73] Consulta realizada en https://sistemas.com/streaming.php el 09/05/2019 a las 4:20 pm
[74] Ley 1712 de 2014, art 6
[75] Ley 1221 de 2008, art 2
[76] Ley 1221 de 2008, art 2
[77] Ley 1581 de 2012, art 3
[78] Consulta realizada en http://www.alegsa.com.ar/Dic/token.php el 09/05/2019 a las 4:50 pm
[79] Decreto 1377 de 2013, art 3

Tratamiento de Datos Personales	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión[80]
Tratamiento del Riesgo	Proceso de selección e implementación de mediciones para modificar el riesgo.[81]
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad[82]
Troyano	Programa ejecutable que aparenta realizar una tarea determinada, para engañar al usuario, con el fin de llevar a cabo acciones como controlar el equipo informático, robar información confidencial, borrar datos, descargar otro tipo de malware, etc. La principal diferencia entre los troyanos y los virus es que los troyanos no pueden replicarse a si mismos.[83]
Usuario	Es la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que haga uso de los servicios ciudadanos digitales.[84] En la PGN se refiere a directivos, funcionarios, contratistas, terceros y otros colaboradores, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Entidad y a quienes se les otorga un nombre de usuario y una contraseña.
Valoración del Riesgo	Totalidad de los procesos de análisis y evaluación de riesgo.[85]
Virus	Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por si mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa y Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.[86]
Vishing	Similar al phising, pero con teléfonos. Consiste en hacer llamadas telefónicas a las victimas, en las que por medio de una voz computarizada, muy similar a las utilizadas por los bancos, se solicita verificar algunos datos personales e información bancaria.[87]

[80] Ley 1581 de 2012, art 3
[81] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 09/05/2019 a las 4:20 pm
[82] ISO/IEC 27000
[83] Consulta realizada en http://www.delitosinformaticos.info/delitos_informaticos/glosario.html el 09/05/2019 a las 4:25 pm
[84] Decreto 1413 de 2017, art 2.2.17.1.3
[85] Consulta realizada en http://www.iso27000.es/download/analisis_ISO-27001.pdf el 09/05/2019 a las 4:20 pm
[86] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:50 pm
[87] Consulta realizada en https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html el 08/05/2019 a las 3:50 pm

VPN	Acrónimo de Virtual Private Network o Red Privada Virtual, en esta forma de comunicación se hace uso de una banda ancha dada por un proveedor en común que actúa como una especie de servidor principal, en la que solo los clientes autorizados pueden tener acceso a los privilegios y servicios que allí se proveen, teniendo una estructura que le permite estar incluida dentro de una red pública, dada su semejanza en diseño y arquitectura.[88]
Vulnerabilidad	Debilidad de un activo o control que pueda ser explotado por una o más amenazas.[89]

[88] Consulta realizada en https://sistemas.com/vpn.php el 09/05/2019 a las 4:45 pm
[89] ISO/IEC 27000