INTRODUCCIÓN

La Alta Dirección de la Procuraduría General de la Nación, entendiendo 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, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Procuraduría General de la Nación, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad, según como se defina en el alcance, a los servidores públicos, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, terceros y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, aprendices, practicantes y clientes de la Procuraduría General de la Nación
- Garantizar la continuidad de la operación frente a cualquier incidente.

La Procuraduría General de la Nación ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

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 solo 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 salvaguardando 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, gracias a la definición, implementación y ejecución efectiva de los controles.
d) Promover una cultura organizacional orientada a la Seguridad de la Información, manteniendo una comunicación asertiva entre la Alta Dirección, los servidores públicos, contratistas y terceros de la Entidad.
e) Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas de la Entidad.
f) Asegurar la continuidad en los procesos de la PGN permitiendo el cumplimiento de los objetivos estratégicos de la Entidad.
g) Cumplir con la legislación colombiana en los temas referentes a la seguridad de la información y a los requerimientos relacionados con la protección de datos personales.
h) Buscar la mejora continua en los procesos asociados a la seguridad de la información.

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 servidores públicos, 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 las 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 las 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 estratégicos, misionales, los de apoyo y los de evaluación y control de la Entidad.

Este compromiso se ve reflejado en la aplicación de la guía de administración de riesgos, en donde se describen las actividades necesarias para identificar y evaluar el nivel de riesgo de los activos digitales de la entidad.

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:

a) 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.
b) Mantener informado al Procurador General de la Nación sobre el estado general de la seguridad de la información de la Entidad.
c) 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.
d) Evaluar y proponer al Procurador General de la Nación, para su aprobación, iniciativas de inversión para incrementar la seguridad de la información.
e) Evaluar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
f) Adoptar los indicadores de gestión de la seguridad de la información.
g) Verificar que la seguridad sea parte del proceso de clasificación de la información.
h) Verificar que la seguridad sea parte del desarrollo de sistemas de información o aplicaciones de software, desde las etapas tempranas del desarrollo.
i) 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 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 servidores públicos, 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.

Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de la entidad, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos según el cargo al que aspira.

Los acuerdos contractuales con contratistas y/o terceros de la entidad, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información, así como un acuerdo de confidencialidad válido aun después de la terminación o cambio de contrato.

Cuando se dé por terminado el contrato o cese la relación laboral el funcionario, contratista y/o tercero debe devolver los activos de información (equipos, documentos, datos), las llaves físicas y de cifrado. Además, la oficina de Tecnología, Innovación y Transformación Digital deberá eliminar los derechos de acceso a los sistemas de información donde esté inscrito el usuario.

La Entidad, a través de la Oficina de Tecnología, Innovación y Transformación Digital, deberá controlar el copiado no autorizado de la información digital por parte de los empleados, contratistas y/o terceros, durante la ejecución del contrato y posterior a la culminación de este. Los líderes del proceso y los designados por el Comité de Seguridad definirán cuál es la información digital no autorizada para su copia.

Durante el periodo de entrega del cargo, se debe asegurar que se documenta la transferencia de la información a la Entidad y posterior borrado seguro de la información, de los medios de almacenamiento removibles y fijos asignados al usuario por parte de la Entidad, previo a la firma del Paz y Salvo por parte del superior inmediato.

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 públicos, 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 los funcionarios públicos y lo hace a través de sus tres funciones misionales principales: la preventiva, de intervención y 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 con 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 que se pueda generar sobre los activos de información, por los riesgos identificados de manera sistemática, a fin 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.

La Entidad debe definir los procedimientos de gestión de políticas de seguridad de la información, para que los responsables del SGSI realicen las actividades necesarias para gestionar y desarrollar nuevas políticas y lineamientos dentro del SGSI. De igual manera, debe establecer las disposiciones que permitan efectuar el control de los documentos y registros del SGSI, a fin de tener disponible la versión vigente de los documentos, para ser utilizada por los usuarios del sistema y facilitar el acceso a esta cuando se requiera.

5.1. Objetivo General del SGSI

Definir en la Entidad lineamientos de acuerdo con lo establecido en el alcance y 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) Implementar el sistema de gestión de seguridad de la información.
e) Proteger los activos de información de la Entidad.
f) Fortalecer la cultura de Seguridad de la Información en los servidores públicos, usuarios, terceros y contratistas de la PGN.
g) Asegurar la continuidad de la operación en la Entidad frente a incidentes de seguridad de la información.
h) Apoyar la innovación tecnológica.
i) Mantener la confianza de los servidores públicos, contratistas y terceros.
j) Cumplir con los principios de la función administrativa.

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. Alcance y Aplicabilidad

Las políticas de seguridad de la información aplican a todos los aspectos administrativos y de control y deben ser cumplidas por sus servidores públicos, contratistas y/o terceros de la Procuraduría General de la Nación y la ciudadanía en general.

5.3. Nivel de Cumplimiento

El cumplimiento de las Políticas de Seguridad de la Información es de carácter obligatorio y cada uno de los servidores públicos, 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 la Información deben ser desarrolladas para ajustarse sin exceder, ni contravenir 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 de la información de la Entidad.

5.4. Principios de Seguridad

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

a) Las responsabilidades frente a la Seguridad de la Información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos, contratistas y/o terceros.
b) La PGN protegerá la información generada, procesada o resguardada por sus procesos, la infraestructura tecnológica y sus activos, del riesgo que se genera de los accesos otorgados a cada uno de los servidores públicos, contratistas y/o terceros.
c) 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.
d) La PGN protegerá las instalaciones de procesamiento de información y la infraestructura tecnológica que soporta sus procesos críticos.
e) La PGN implementará controles asociados a la operación de sus procesos misionales propendiendo por la seguridad de la infraestructura tecnológica.
f) La PGN implementará controles de acceso a los activos de información, de acuerdo con su nivel de clasificación.
g) 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.
h) 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.
i) La PGN propenderá por el cumplimiento del ordenamiento legal, regulatorio y contractual establecido.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

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 y son la base para la definición e implementación de los controles, procedimientos y estándares, y por lo tanto deben ser 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 - TI-PO-03

La Procuraduría General de la Nación define las reglas para el acceso controlado a la información, ya sea de forma física o lógica.

La Oficina de Tecnología, Innovación y Transformación Digital de la PGN establece la *Política Específica para el Control de Acceso,* para los sistemas de Información y el Centro de Procesamiento de Datos, además de la asignación de los derechos de acceso de los usuarios a los recursos de la Entidad, teniendo en cuenta los requisitos y los niveles de seguridad lógicos y físicos establecidos.

El control de acceso a la información se implementa bajo el principio del mínimo privilegio que el funcionario, contratista y/o tercero requiera para el desarrollo de sus actividades diarias. La información se cataloga de acuerdo con los niveles de clasificación definidos en la *Política Específica de Gestión y Clasificación de Activos de Información*, y se accede según el perfil asignado al usuario.

6.2. Política de Uso Aceptable de Equipos de Cómputo - TI-PO-09

La Procuraduría suministra a los servidores públicos los recursos informáticos con el único fin de desarrollar las actividades relacionadas a su cargo y dentro del contexto de la Entidad, de acuerdo con los criterios establecidos en el *Manual específico de funciones y de requisitos por competencias laborales MC-M-01* de la Entidad, por lo cual estos recursos deben ser utilizados de forma adecuada y eficiente.

Es responsabilidad de los servidores públicos, hacer buen uso del equipo y los servicios de cómputo asignados, así como salvaguardar la seguridad de la información que se encuentre almacenada en medios magnéticos, medios ópticos, equipos de cómputo de escritorio, escritorios virtuales, portátiles y demás repositorios de almacenamiento, tanto fijos como extraíbles asignadas al funcionario.

Las directrices para la seguridad en el uso de los equipos de cómputo se encuentran definidas en la *Política Específica de Uso Aceptable de Equipos de Cómputo.*

6.3. Política de Uso de Recursos y Servicios Tecnológicos - TI-PO-10

La PGN brinda a sus servidores públicos, contratistas y/o terceros una serie de servicios tecnológicos para la realización de sus respectivas actividades laborales. Estos recursos deben ser utilizados exclusivamente para dichas actividades.

El servicio de internet y el correo electrónico institucional son herramientas de apoyo a las funciones y responsabilidades de los servidores públicos 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 directrices relacionadas en el documento de *Política Específica de Uso de Recursos y Servicios Tecnológicos*.

La PGN tiene instalado, 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 usuarios, 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 malware, buscando infectar los equipos o sustraer información personal obteniendo los datos de los usuarios en alguna página fraudulenta; a fin de que esto suceda, los servidores públicos, contratistas y/o terceros deben seguir las indicaciones de seguridad para el uso de Internet listados en el Anexo A del documento de *Política Específica de Uso de Recursos y Servicios Tecnológicos.*

La Oficina de Tecnología, Innovación y Transformación Digital 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 Tecnología, Innovación y Transformación Digital podrá restringir su acceso hasta tanto se normalice el servicio.

Es función de la Oficina de Tecnología, Innovación y Transformación Digital 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 de este servicio, que pueda 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 servidores públicos 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.

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

La Oficina de Tecnología, Innovación y Transformación Digital es la 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.

Así mismo, es la responsable de instalar el sistema antimalware en cada dispositivo de cómputo incluyendo los servidores on-premise o en la plataforma de un proveedor en la nube; debe utilizarse únicamente este software licenciado para la revisión y verificación de malware en los equipos y archivos, y los servidores públicos no deben desactivar, alterar o desinstalar el aplicativo instalado para este fin. La oficina de Tecnología, Innovación y Transformación Digital debe garantizar que los usuarios no puedan realizar ninguna de las actividades indicadas.

La Oficina de Tecnología, Innovación y Transformación Digital 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 malware 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 software malicioso al interior de la red. Para mayor control de antimalware se debe aplicar la *Política Específica de Uso de Recursos y Servicios Tecnológicos*.

6.4. Política de Escritorio y Pantalla Limpia - TI-PO-13

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 servidores públicos de la PGN cumplirán con los lineamientos definidos en el documento de *Política Específica de Escritorio y Pantalla Limpia*.

Para proteger la seguridad de la información que se envía a las impresoras, el personal asignado por la Oficina de Tecnología, Innovación y Transformación Digital verificará que las impresoras que tienen soporte para conexión directa a la red cumplan con las siguientes indicaciones:

a) Se encuentren conectadas en los segmentos de red institucionales correspondientes.
b) Si cuentan con la funcionalidad, el acceso a su panel de configuración debe ser mediante contraseña y su tráfico debe ir cifrado.
c) Si están conectadas por WIFI se debe configurar su seguridad y cifrado.
d) Los discos duros de las impresoras deben revisarse periódicamente, con el fin de eliminar la información sensible que allí haya quedado almacenada después de la impresión.
e) Si cuentan con la funcionalidad de bloqueos de puertos USB, estos deben estar deshabilitados.
f) Siempre que sea posible, se debe disponer de mecanismos de impresión segura (con contraseña).
g) El usuario debe recoger inmediatamente aquellos documentos enviados a imprimir. No se deben dejar documentos en la impresora al finalizar el día de trabajo o al receso de almuerzo.

6.5. Política de Dispositivos Móviles - TI-PO-06

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 servidores públicos hagan un uso responsable de los servicios, equipos y aplicativos disponibles en la Entidad.

La asignación de los dispositivos móviles a los servidores públicos 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 Tecnología, Innovación y Transformación Digital, o al Coordinador del Grupo de Infraestructura, por parte del interventor del contrato o profesional responsable de las actividades del contratista o proveedor de servicios.

La Oficina de Tecnología, Innovación y Transformación Digital es la 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.

El documento *Política Específica de Dispositivos Móviles* define los lineamientos que deben seguir los servidores públicos, contratistas y/o terceros con relación al uso de los dispositivos móviles, y el documento *Política Específica de Escritorio y Pantalla Limpia*, presenta las indicaciones para no dejar desatendidos dichos dispositivos.

Los servidores públicos deben tener en cuenta los lineamientos definidos en la *Política Específica de Control de Acceso*, con respecto al tema de la gestión de contraseñas y el acceso a la red de los dispositivos móviles.

La sincronización de la cuenta de correo electrónico institucional en el dispositivo móvil de uso institucional debe ser realizada por los profesionales designados por la Oficina de Tecnología, Innovación y Transformación Digital de la Entidad.

La sincronización de la cuenta de correo electrónico institucional, en los dispositivos móviles de uso personal, deberá contar previamente con la configuración del doble factor de autenticación o los mecanismos que cumplan con la misma funcionalidad. En el caso que el usuario necesite apoyo para la configuración del dispositivo móvil, lo debe solicitar a través de los diferentes canales de la Mesa de Servicios.

Las computadoras portátiles que ingresen y/o salgan de las instalaciones de la PGN deben ser registradas 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.

Los equipos personales o portátiles 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 la Mesa de Servicios.

Para mayor seguridad de los dispositivos móviles se debe dar cumplimiento, por parte de los servidores públicos, contratistas y terceros, al Anexo A del documento de *Política Específica de Dispositivos Móviles*.

6.6. Política de Teletrabajo y Trabajo en Casa - TI-PO-05

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 y Trabajo en Casa a los servidores públicos asignados.

Dentro del documento Acuerdo de Teletrabajo, se consignan las obligaciones de la PGN y las obligaciones generales de los servidores públicos, 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 servidores públicos que hacen parte de este.

Debido a esto, la PGN amplía la política para incluir dentro de las políticas de seguridad de la información las actividades asociadas al trabajo en casa, la cual define los lineamientos para ambos tipos de actividades en el documento de *Política Específica de Teletrabajo y Trabajo en Casa*.

Las conexiones establecidas para el acceso remoto, ya sea por la modalidad de teletrabajo o de trabajo en casa se deben realizar siguiendo los lineamientos definidos en la *Política Específica de Control de Acceso*, buscando un acceso remoto seguro.

6.7. Política de Transferencia de Información - TI-PO-11

La transferencia de información es un proceso requerido en las actividades de la PGN y, por lo tanto, deberá realizarse protegiendo la confidencialidad, disponibilidad e integridad de los datos de acuerdo con la clasificación del tipo de información involucrada. La clasificación se determina siguiendo los lineamientos definidos en la *Política Específica de Gestión y Clasificación de Activos de Información*, teniendo en cuenta las clasificaciones definidas en el Anexo A.

El documento de *Políticas Específicas de Transferencia de la Información* determina los lineamientos que se deben seguir para la transferencia de información física y/o digital, ya sea internamente entre servidores públicos de la PGN o con terceros.

6.8. Política de Uso de Controles Criptográficos y Gestión de Llaves Criptográficas - TI-PO-12

La PGN clasifica la información teniendo en cuenta diferentes aspectos, como se define en el Anexo A de la *Política Específica de Gestión y Clasificación de Activos de Información*.

La Información Pública Nacional, clasificada como pública reservada o pública clasificada debe ser cifrada siguiendo los lineamientos definidos en la *Política Específica de Uso de Controles Criptográficos y Gestión de Llaves Criptográficas*.

Cuando se habla de información que no es Pública Nacional y que se clasifica como Alta o Media en el Nivel de Clasificación General definido en el Anexo A de la *Política Específica de Gestión y Clasificación de Activos de Información*, se hace referencia a:

a) Bases de datos, registros de usuarios, correos electrónicos confidenciales
b) Información sujeta a protección legal
c) Backups
d) Información confidencial en dispositivos extraíbles y móviles
e) Credenciales de acceso
f) Credenciales para pagos online
g) Sistema de gestión documental

Por su trascendencia e importancia la información debe estar especialmente protegida tanto en tránsito como cuando está almacenada, siguiendo los lineamientos definidos en la *Política Específica de Uso de Controles Criptográficos y Gestión de Llaves Criptográficas*. y la *Política Específica de Control de Acceso*.

Para proteger esta información, además de controlar el acceso a la misma y proteger los sistemas con los que se manejan, se deben cifrar los datos a través de herramientas criptográficas, 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.

Para la gestión documental electrónica, para garantizar el no repudio de datos, se requiere disponer de los siguientes certificados:

a) Certificado Digital de Persona Jurídica.
b) Certificado de Servidor Seguro (SSL).
c) Correo Electrónico Certificado.
d) Estampado Cronológico.

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 se deben usar mecanismos de estampado cronológico, aplicándolos con todos los documentos que se reciben, radican, digitalicen y sean 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 servidores públicos 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 del sitio 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.

Para establecer el sistema de cifrado, se tiene en 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:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
b) Definir el protocolo para activar y recibir las llaves y su distribución a los usuarios autorizados y el periodo de activación de esta.
c) Definir criterios para el almacenamiento de las llaves y la forma de acceso por parte de los usuarios autorizados.
d) Definir criterios para el cambio o actualización de las llaves.
e) Revocar las llaves cuando se han puesto en peligro o cuando se retira el funcionario de la Entidad.

f) Definir criterios para archivar las llaves y para destruirlas.
g) Definir procedimiento para recuperar llaves pérdidas o corruptas.
h) Mantener registros de auditoría de las actividades de gestión de llaves
i) La caducidad de las llaves criptográficas públicas de los terceros será potestad de ellos y acogida por la PGN
j) Sera responsabilidad del tercero actualizar sus llaves criptográficas públicas e informar a la Entidad para su actualización.
k) 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.

La gestión de claves criptográficas debe seguir los lineamientos definidos en la *Política Específica de Uso de Controles Criptográficos y Gestión de LIaves Criptográficas*.

Las conexiones establecidas de forma remota deben realizarse a través de comunicaciones cifradas vía VPN como se determina en el documento de *Política Específica de Controles de Acceso*.

6.9. Política de Copias de Seguridad - TI-PO-07

La PGN adoptará prácticas de Copias de Respaldo o Backup para garantizar la disponibilidad de la información y la continuidad de las operaciones de la entidad.

La PGN debe disponer del procedimiento para realizar Copias de Respaldo o Backup, así como la restauración de los datos que se almacenan en los equipos servidores de la Entidad, a fin de mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de esta.

Los instructivos de respaldo y restauración deben permitir:

a) Determinar el nivel de criticidad de la información y el periodo de retención de las copias de respaldo.
b) Realizar registros exactos y completos de las copias.
c) Estipular la extensión y frecuencia de los respaldos, que indique los requisitos de seguridad de la información y la importancia de la operación.
d) Indicar 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: Solo se graban los datos que han cambiado desde la última copia;
- Diferencial: Se copian los datos que han cambiado desde la última copia

completa.

e) Que el respaldo de información confidencial se proteja por medio de cifrado.

Para el respaldo y recuperación segura de la información, la PGN debe adoptar y dar cumplimiento a los lineamientos que en materia de copias de respaldo de la información suscriba.

Los lineamientos para la gestión de las copias de seguridad y la realización de los respaldos se encuentran definidos en la *Política Específica de Copias de Seguridad*.

6.10. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información - TI-PO-02

La PGN establece e implementa 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 o al interior de la Entidad a los sistemas de información.

Se debe asegurar la confidencialidad, disponibilidad, integridad y no repudio de la información que se encuentra almacenada en las bases de datos de los diferentes sistemas de información, por esta razón, 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.

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

a) Se deben identificar, justificar, acordar y documentar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software.
b) Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
c) 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 el caso que se deba dar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
d) 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.
e) Los ambientes de desarrollo, pruebas, capacitación y producción deben estar separados.
f) 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.

g) El ambiente de pruebas 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.
h) 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.

En el documento de Políticas Específicas de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, se definen los lineamientos para la seguridad del ciclo de vida del desarrollo de software, el cual incluye los procesos de adquisición de software a un tercero, desarrollo interno o de un tercero y mantenimiento del sistema de información.

6.11. Política de Gestión de Incidentes de seguridad del a información - TI-PO-14

La PGN adopta 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 de la Entidad, cumpliendo con las directrices de las normas ISO 27001:2013 y el estándar ISO 27035 sobre gestión de incidentes de seguridad.

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

a) Incidentes no intencionados o involuntarios
b) Daños físicos
c) Incumplimiento o violación de requisitos y regulaciones legales
d) Fallos en las configuraciones
e) Denegación de servicio
f) Acceso no autorizado, espionaje y robo de información
g) Borrado o pérdida de información
h) Infección por software malicioso.

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

a) Detectar, reportar y evaluar incidentes de seguridad de la información.
b) Responder a incidentes de seguridad de la información, incluida la activación de controles adecuados para la prevención y la reducción de impactos.
c) Reportar las vulnerabilidades de seguridad de la información, evaluarlas y tratarlas adecuadamente.

d) 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.

Los lineamientos asociados a la gestión de incidentes de seguridad de la información se encuentran definidos en el documento de *Política Específica de Gestión de Incidentes de Seguridad de la Información*.

6.12. Política de Gestión y Clasificación de Activos de Información - TI-PO-04

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 servidores públicos indicaciones sobre el uso apropiado de los activos de información con el propósito de proteger a la Entidad y sus activos de información.

La oficina de Tecnología, Innovación y Transformación Digital en conjunto con los responsables de los procesos deberán identificar, clasificar, etiquetar, disponer, valorar y gestionar los activos de información de acuerdo con el 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 el procedimiento *DO-P-11 Identificación y Clasificación de Activos de Información*.

Los lineamientos para la clasificación de los activos de información se encuentran definidos en el documento de *Política Específica de Gestión y Clasificación de Activos de Información*.

6.13. Política de Relación con Proveedores - TI-PO-08

Los Proveedores deben garantizar que los activos de información que van a estar bajo su responsabilidad cuenten con las medidas de seguridad definidas en las políticas de seguridad de la información.

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

El documento de *Política Específica de Relación con Proveedores* determina los lineamientos que se deben seguir en los procesos asociados a la contratación, acuerdos, seguimiento de los servicios brindados por los diferentes proveedores de la PGN. También se deben tener en

cuenta los lineamientos definidos en las diferentes políticas de seguridad, que apliquen a los proveedores de la PGN.

7. FASES DE IMPLEMENTACIÓN

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

7.1. Desarrollo

En esta fase se definen 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 servidores públicos, 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

La Entidad debe destinar los recursos necesarios para la implementación, mantenimiento y cumplimiento de las políticas específicas de Seguridad.

7.3. Comunicación

En esta fase se da a conocer a todos los servidores públicos, contratistas y/o terceros las políticas específicas 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 se debe medir y determinar la efectividad y cumplimiento de las políticas específicas de Seguridad de la Información mediante mecanismos de monitoreo (p. e. indicadores, métricas, auditorías internas y externas).

7.5. Mantenimiento

En esta fase la PGN debe asegurar que las políticas específicas 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 aplicará mecanismos de eliminación, previamente definidos, a las políticas específicas de Seguridad de la Información que 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. 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 revisión permite garantizar que los documentos sigan estando vigentes y alineados con la realidad. La revisión debe quedar consignada en la hoja control de documentos así no se hayan realizado cambios en este.

La fecha de vigencia de las Políticas de Seguridad de la Información será a partir de su aprobación por parte del Comité Institucional de Gestión y Desempeño.

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.

Los lineamientos asociados a la realización de cambios en las políticas de seguridad de la información se encuentran definidos en el documento denominado procedimiento de Gestión de Políticas de Seguridad de la Información.

9. TÉRMINOS Y 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. Aquellos que no se encuentren definidos a continuación, deben entenderse con su significado natural.

Activo de Información: Colección de datos relacionados y representados por símbolos que tienen valor para la Entidad y que se encuentran en formato físico o digital, que han sido generados o transformados por algún proceso manual o computacional y que sirven como materia prima para el cumplimiento de los objetivos de la Organización y para la toma de decisiones.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a un proceso de la Entidad.

Antimalware: Antimalware es una categoría de software de seguridad que protege un equipo de malware, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina el software malicioso. El antimalware debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Apetito del riesgo: Nivel de riesgo que la entidad está dispuesta a asumir.

Archivo: Documento físico o digital, 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.

Autenticidad: Característica de los activos de información que permite validar que este es un recurso legítimo y que sus propiedades no han sido manipuladas sin autorización.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Capa de Sockets Seguros (SSL): Está compuesta por un conjunto de protocolos de comunicaciones que hacen uso de la criptografía para asegurar la confidencialidad de las comunicaciones entre dos computadoras.

Certificado de Servidor Seguro (SSL): 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.

Certificado 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.

Ciberseguridad: Conjunto de esfuerzos, personas, tecnologías y demás recursos dispuestos por la Entidad para proteger sus activos de información reduciendo el nivel de riesgo de estos con el fin de que no se vean afectados por amenazas digitales.

Cifrado: Mecanismo a través del cual se emplean algoritmos computacionales que hacen uso de funciones matemáticas complejas y una o un par de llaves utilizadas para proteger la confidencialidad de la Información digital.

Clasificación de la Información: Es el ejercicio por medio del cual se determina el nivel de relevancia de los activos de información para la Entidad en términos de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que el activo de información recibe el nivel de protección adecuado.

Confidencialidad: Característica primaria de los activos de información referente a que estos solo sean accedidos por personas autorizadas por la Entidad.

Contraseña: Cadena de caracteres, símbolos y números asignados a un usuario como parte de sus credenciales, que es utilizada por uno o varios sistemas computacionales para identificar una cuenta y determinar los privilegios que esta posee para hacer uso de los recursos tecnológicos de la Entidad (Acceso a un sistema de información, al sistema operativo, etc.).

Control: Conjunto de contramedidas administrativas y técnicas como son las políticas, los procedimientos, las personas, tecnologías, prácticas y las estructuras organizativas concebidas y desplegadas para tratar de modificar el riesgo de seguridad de la información o de mantenerlo por debajo del apetito del riesgo de la Entidad.

Correo Electrónico Certificado: Mensaje de correo electrónico que esta soportado por un servicio de notificación electrónica que cuenta con la misma validez jurídica y probatoria que un envío certificado por medios físicos y con mayores fortalezas funcionales, técnicas y jurídicas que los mensajes electrónicos convencionales o no certificados.

Correo Electrónico Institucional: Es el servicio de correo electrónico que provee y administra directamente la Procuraduría General de la Nación a sus usuarios, como herramienta de apoyo a las funciones y responsabilidades de estos.

Cuenta de usuario: Cadena de texto utilizada para representar a un usuario (persona) dentro de un sistema computacional o un sistema de información. Generalmente esta complementado con una contraseña (que no debe ser compartida).

Disponibilidad: Propiedad de los activos de información que debe garantizar que estos sean accesibles y utilizables por los usuarios que cuenten con legitima autorización para esto, cuando las necesidades del servicio así lo requieran.

Dispositivo Móvil: Un dispositivo móvil se puede definir como un sistema computacional portable generalmente de menor tamaño que una computadora de escritorio, con capacidades de procesamiento, con conexión permanente o intermitente a una red de comunicaciones generalmente de forma inalámbrica.

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.

Evaluación de Riesgo: Proceso en el cual se comparan los riesgos estimados o calculados, contra los criterios de riesgo establecidos por la metodología de gestión de riesgos elegida por la Entidad, para determinar el nivel de severidad que podría representar la materialización de las amenazas previamente identificadas.

Firma Digital: archivo/cadena cifrada con criptografía asimétrica que puede adherirse a un mensaje de datos y que, utilizando un procedimiento matemático complejo, vincula a la clave pública del emisor del mensaje y al mensaje en sí mismo con dicho emisor, garantizando que este mensaje realmente ha sido enviado por el emisor conocido y que este no ha sido modificado después de ser firmado.

Gestión de Incidentes de Seguridad de la Información: Proceso para detectar, identificar, evaluar, tratar, responder, notificar y aprender de los incidentes de seguridad de la información que puedan presentarse en la Entidad.

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.

Incidente de Seguridad de la Información: Evento o conjunto de eventos de seguridad de la información resultantes de la materialización de por lo menos una amenaza sobre uno o varios activos de información de la Entidad.

Información: Resultado del procesamiento y organización de un conjunto de datos como parte de un proceso de la Entidad. La información puede estar contenida en cualquier documento

físico o digital que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal y que su exposición/publicación no afecte la seguridad de la información de la Entidad.

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.

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.

Integridad: Característica primaria de los activos de información referente a que las modificaciones solo puedan ser realizadas por los usuarios legítimos durante el periodo de tiempo autorizado por la Entidad

Inventario de Activos: Lista de todos aquellos activos de información de la Entidad, dentro de los cuales se encuentran los archivos, bases de datos, registros, software, documentos, servicios, personas, etc., que se encuentran dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Malware: Producto de software construido con el fin de afectar la confidencialidad y/o integridad y/o disponibilidad de los activos de información digital.

No Repudio: Es un atributo deseado de todas las transacciones que brinda protección contra la negación de responsabilidad por parte de las partes que intervienen en un trámite de la Entidad.

Phishing: Ataque informático de suplantación de identidad basado en ingeniería social apoyada en computación y frecuentemente utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como pueden ser credenciales de acceso, información sobre tarjetas de crédito u otra información bancaria de la víctima, entre otras; para posteriormente abusar de estas.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman flujos de entrada (generalmente colecciones de datos) en flujos de salida (Información).

Propietario de Activo de Información: Persona, parte designada de la entidad, o grupo de trabajo que tiene la responsabilidad de salvaguardar la seguridad de los activos de información que están a su cargo.

Proveedor de Redes y Servicios: Persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros.

Publicar o Divulgar: Significa poner a disposición uno o varios activos de información, en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión.

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.

Seguridad de la Información: Conjunto de políticas, procedimientos, personas y demás recursos dispuestos por la Entidad para tratar de preservar la confidencialidad, integridad y disponibilidad de sus activos de información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de procesos, estructura organizativa, políticas, actividades, responsabilidades, procedimientos y recursos que dispone una organización para proteger a sus activos de información, estableciendo una política y unos objetivos de seguridad orientados a reducir los riesgos, basándose en un enfoque de gestión permanente y de mejora continua.

Spam: También conocido como correo basura, se llama spam a los mensajes de correo electrónico que pretenden suplantar a mensajes legítimos 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 que posteriormente serán destinatarios de mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

Sujetos Obligados: Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5 de la Ley 1712 de 2014.

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.

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.

Trabajo en Casa: El trabajo en casa permite que los empleadores autoricen a sus trabajadores ante una situación ocasional temporal y excepcional a realizar sus labores desde su lugar de residencia como alternativa para el desarrollo de actividades.

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.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

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

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. En la PGN se refiere a directivos, servidores públicos, 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 una cuenta de usuario de usuario y una contraseña.

VPN: Acrónimo de Virtual Private Network o Red Privada Virtual, es un conjunto de tecnologías que incluye protocolos de comunicaciones y algoritmos de cifrado para proteger las comunicaciones digitales de extremo a extremo, que se realizan sobre redes públicas como Internet.

Vulnerabilidad: Debilidad de un activo de información, sistema computacional, control, persona o proceso que pueda ser explotado por una o más amenazas.

10. CONTROL DE CAMBIOS

FECHA	VERSIÓN DEL DOCUMENTO QUE MODIFICA	DESCRIPCIÓN DEL CAMBIO
30/10/2019	1	Creación de la Política de seguridad de la Información adoptada mediante Resolución 910 del 25 de septiembre de 2019.
31/07/2022	2	Teniendo en cuenta lo dispuesto en el memorando 005 del 22 de julio de 2022, referente a la “Implementación y mantenimiento del Sistema de Gestión de Calidad – SGC”, se actualiza este documento conforme a los lineamientos establecidos para la gestión de la información documentada, se aplica la nueva plantilla y su codificación toda vez que este documento se encontraba identificado con el código POL-GT-00-001.
25/01/2024	3	Se ajusta la política definiendo una política general de la seguridad de la información y se definen las políticas específicas por temática.