FISCALIA
GENERAL DE LA NACIÓN

RESOLUCIÓN No. 0 4004

06 NOV. 2013

Por la cual se actualizan las políticas de seguridad de la información, emitidas mediante la Circular DFGN – 0001, mayo 6 de 2006 del Fiscal General de la Nación.

EL FISCAL GENERAL DE LA NACIÓN

En uso de sus atribuciones legales y en especial las que le confiere el numeral 17 del artículo 11 de la Ley 938 del 30 de diciembre de 2004, y

CONSIDERANDO

Que de conformidad con la Ley 938 de 2004, Artículo 22, numeral 1... *"corresponde a la Oficina de Informática el asesorar al Fiscal General de la Nación en la definición de las políticas referidas a la gerencia de los recursos informáticos y telemáticos disponibles en la entidad..."*

Que de conformidad con la Ley 938 de 2004. Artículo 22, numeral 8..."*corresponde a la Oficina de Informática elaborar e implantar políticas, planes y programas para el desarrollo informático y telemático de la Fiscalía General de la Nación...*".

Que de conformidad del artículo 22 numerales 1 y 8 del Decreto 2699 de noviembre 30 de 1991..."*El Fiscal General de la Nación tendrá la representación de la entidad frente a las autoridades del Poder Público así como frente a los particulares y cumplirá las siguientes funciones: 1. Expedir reglamentos, órdenes, circulares y los manuales de organización y procedimientos conducentes a la organización administrativa y al eficaz desempeño de las funciones de la Fiscalía General de la Nación.... 8. Expedir los Manuales de Procedimiento Administrativo y de normas técnicas a que se deben someter a los funcionarios de la Fiscalía General y la Policía Judicial en el cumplimiento de sus funciones...*".

Que las normas y políticas de seguridad informática en la Fiscalía General de la Nación se encuentran enmarcadas en preceptos Constitucionales, Leyes, Decretos, Convenios Internacionales, así como en Resoluciones, Circulares y Memorandos proferidos por la Entidad. Entre las que se encuentran:

a. Ley de Delitos Informáticos. *Ley 1273 de Enero de 2009.*

b. Ley de Correo Electrónico: *Ley 527 de 1999.*

c. Decreto 1747 del 2000: Por *el cual se reglamenta parcialmente la Ley 527 de 1999.*

d. Ley General de Archivo: *Ley 594 de 2000 - El Párrafo 1 del artículo 19..." establece la obligación de garantizar la autenticidad, integridad y la inalterabilidad de la información allí consignada..."*

e. Código de Ética y Buen Gobierno: Adoptado *mediante Resolución Nº 0-6552 del 24 de Octubre de 2008. – Capítulo VI: De los Valores Institucionales – De las directrices para la Gestión Ética: Artículos 2 y 21.*

f. Código sustantivo del trabajo: Artículo 58. – Obligaciones Especiales del Trabajador, 3ª:..*"Conservar y restituir en buen estado, salvo el deterioro natural, los instrumentos y útiles que le hayan sido facilitados y las materias primas sobrantes…".*

g. Ley de Derechos de Autor: Ley 23 de 1982.

h. Ley de Habeas Data: Ley 1266 de Diciembre de 2008.

Con respecto al tema relacionado con la legislación aplicable a la frase "*todo funcionario debe proteger y salvaguardar los activos de la empresa para la que trabaja como si fueran propios*", se tienen las siguientes leyes:

a. Constitución Política de 1991, artículo sexto.

b. Código Civil Colombiano, artículo 63.

c. Ley 970 de 2005, artículo 1 y 12.

d. Ley 734 de 2002 Código Único Disciplinario, artículo 35.

e. Ley 842 de 2003, artículo 31, literal b.

f. Ley 610 de 2000, artículo 3.

g. Ley 87 de 1993 y sus modificaciones.

h. Ley 42 de 1993, artículo 107.

Que la Fiscalía General de la Nación suministra a sus empleados, funcionarios y terceras partes, servicios y recursos informáticos, basada en la necesidad de mantenerse a la par con los nuevos adelantos tecnológicos que contribuyan al logro de sus objetivos misionales.

Que la información generada por la Fiscalía General de la Nación y la tecnología informática que la soporta, se han convertido en elementos absolutamente indispensables para el funcionamiento de la Entidad, de tal manera que junto con el capital humano, es necesario protegerlos contra toda una serie de eventualidades que pueden atentar contra el objetivo de la Fiscalía de garantizar el acceso a una justicia oportuna y eficaz.

Que dichas eventualidades pueden ser causadas por factores naturales, como un incendio, una inundación, o factores tecnológicos, tales como fallas en un equipo de cómputo o incluso factores humanos, como por ejemplo, una acción accidental o malintencionada que provoque la interrupción prolongada de los servicios informáticos, la modificación de la información almacenada o el ingreso de personas o grupos no autorizados a los sistemas de información de la Entidad.

Que con la implementación y utilización de soluciones tecnológicas por parte de la Fiscalía General de la Nación, para facilitar el logro de su misión, visión, objetivos y direccionamiento estratégico, se cuenta hoy en día con una importante infraestructura informática que requiere del diseño, la implementación y seguimiento de normas de seguridad informática que contribuyan a mantener la integridad, confidencialidad y disponibilidad de la información, protegiéndola de ataques provenientes de Internet, de redes de otras entidades con quienes se intercambia información institucional logrando con ello minimizar el impacto ante posibles ataques presentados al interior de la organización.

Que es necesario garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad.

Que de acuerdo al contenido de la estrategia de Gobierno en Línea en sus componentes "Elementos Transversales: En este componente también se describen actividades orientadas a que cada entidad cuente con una política de seguridad que es aplicada de forma transversal y mejorada constantemente"

Que por las razones anteriores, la Fiscalía General de la Nación ha establecido una política de seguridad informática y normas de seguridad como parte de la cultura organizacional de la entidad para dar respuesta a las necesidades de protección de los activos informáticos, las cuales han sido complementadas con la adquisición y actualización de soluciones informáticas de seguridad, así como el compromiso manifiesto de la alta dirección de la Fiscalía General de la Nación para la difusión, consolidación y cumplimiento de dichas políticas, por parte de todos los usuarios que utilizan los recursos informáticos de la Entidad.

Que en mérito de lo expuesto,

RESUELVE:

ARTICULO PRIMERO.- OBJETIVO.

La política de seguridad informática tiene por objetivo proteger los activos informáticos de la Fiscalía General de la Nación y garantizar un adecuado uso de la tecnología, ante amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

ARTICULO SEGUNDO.- ALCANCE.

La Política General de Seguridad informática establece los lineamientos de gestión adecuada para el uso de los activos informáticos de la Entidad, asegurando la implementación de los controles y medidas de seguridad formuladas en esta Política a partir de la identificación de los activos informáticos, las partidas presupuestarias correspondientes y el cumplimiento de las disposiciones legales vigentes.

Por tal razón, esta Política debe ser continuamente actualizada de acuerdo con los procesos, procedimientos, instructivos y actividades establecidos en la Entidad, a efectos de asegurar su vigencia y nivel de eficacia, así como conocida y cumplida por todos los

usuarios de los activos informáticos, es decir servidores, contratistas y terceras personas que de alguna forma tengan acceso a los recursos informáticos de la Fiscalía General.

Lo anterior en coherencia con las normas planteadas en este documento y con las Políticas de Seguridad Informática elaboradas en el marco de la Norma Técnica Colombiana NTC-ISO/IEC 27001, así como con los documentos de procedimientos y recomendaciones que se han publicado y formalizado mediante Resolución 2287 del 5 de noviembre de 2003, y de los lineamientos del SGC y MECI.

ARTICULO TERCERO.- TERMINOS Y DEFINICIONES.

Acceso Remoto: Sistema externo que permite conectarse a la red de computadores de la Entidad.

Activo informático: Se refiere a la infraestructura de TIC y todo lo relacionado con esta.

Antimalware: Aquel software que evita la infiltración en el sistema y el daño.

CCTV: Video-vigilancia, conocido como Circuito Cerrado de Televisión. El video-vigilancia es un sistema de tecnología de vigilancia con cámaras.

Confidencialidad: Es la propiedad de un documento o mensaje que únicamente está autorizado para ser leído o entendido por personas o entidades autorizadas.

Cuenta de Usuario (usuario): Es un conjunto de permisos, recursos y privilegios a los que se tiene acceso mediante el registro previo de una cuenta la cual es asignada a los servidores públicos de la FISCALÍA GENERAL DE LA NACIÓN y terceros, es decir todo aquel que requiera hacer uso autorizado de los recursos informáticos de la FISCALÍA GENERAL DE LA NACIÓN.

Disponibilidad: Es garantizar que los recursos informáticos puedan ser utilizados por quien los necesite y cuando los necesite.

Escritorio remoto: Es la tecnologia que permite que un equipo (cliente) se conecte a equipo remotamente (anfitrión). Los equipos pueden estar ubicados en geográficamente diferentes lugares.

Incidente de Seguridad: Es un evento que atenta contra la Confidencialidad, Integridad y Disponibilidad de la información y los activos informáticos de la *FISCALÍA GENERAL DE LA NACIÓN*.

Integridad: Propiedad de la información de ser completa y veraz.

Mensajería Electrónica: Son los servicios tecnológicos utilizados para el intercambio de mensajes de forma electrónica; el ejemplo típico es el correo electrónico o e-mail.

Normatividad: Indica los requisitos específicos de índole legal y técnico establecidos para el cumplimiento de las políticas de seguridad informática.

Entre las normas de seguridad informática internacionales más utilizadas se tienen:

- NORMA NTC – ISO/BS 7799
- NORMA NTC – ISO/IEC 17799
- NORMA NTC – ISO/IEC 27000
- NORMA NTC – ISO/IEC 27001:2005
- NORMA NTC – ISO/IEC 27002
- NORMA NTC – ISO/IEC 38500:2008

NTC-ISO/IEC 27001: Norma internacional que define un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Oficial de seguridad: El Oficial de seguridad informática (OSI), es la persona responsable de planear. coordinar y administrar los procesos de seguridad informática en una organización.

Políticas de Seguridad de la Información: Es el conjunto de responsabilidades generales aplicables a toda la entidad en lo que respecta al uso adecuado de los activos para la gestión de la información.

Proxy: Punto intermedio entre un ordenador conectado a Internet y el servidor que está accediendo.

Redes: Son los dispositivos y medios utilizados para transferencia electrónica de datos.

Seguridad de la Información: Todos los aspectos relacionados con la definición, el logro y el mantenimiento de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sniffers: Técnicamente es un programa informático que registra la información que envían los periféricos de una red para poder monitorear la actividad de un determinado ordenador.

Software: Es el conjunto de programas y aplicaciones en un sistema informático necesarios para hacer posible la realización de una tarea específica.

Spam: es el hecho de enviar mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas.

Terceros: Son todos aquellos entes externos o personas que no son funcionarios públicos de la *FISCALÍA GENERAL DE LA NACIÓN*, pero tienen acceso autorizado a los recursos informáticos de la Entidad, como los son entre otros: Contratistas autorizados, judicantes, estudiantes en pasantías y funcionarios de otras entidades autorizados por Ley, por convenio, contrato u orden de servicio.

TIC: Tecnología de la Información y las comunicaciones.

VPN (Virtual Private Network): O red Privada Virtual, es una tecnología de red que permite extender de manera segura los servicios de una red privada (como la de la Fiscalía) sobre una red pública (como Internet).

ARTICULO CUARTO.- SEGURIDAD INFORMÁTICA.

La política de seguridad informática se constituye en la primera linea de defensa de la entidad frente a amenazas sobre la información institucional, ya que su construcción está basada en un proceso continuo de análisis de riesgos y de la implementación de controles apropiados para la mitigación de posibles daños con el fin de garantizar la disponibilidad, confidencialidad e integridad de los activos informáticos, en el cumplimiento de los objetivos de la Entidad.

ARTICULO QUINTO.- DECLARACION DE POLITICA DE SEGURIDAD.

Todos los empleados y funcionarios de la FISCALÍA GENERAL DE LA NACIÓN, así como terceros que deban realizar labores por medios lógicos o físicos que involucren el manejo de información de la Entidad, deben velar por la disponibilidad, confidencialidad e integridad de los activos informáticos, cumpliendo con las políticas de seguridad establecidas y las correspondientes cláusulas de confidencialidad de la información que para su caso aplique.

5.1. SEGURIDAD ORGANIZACIONAL.

Gestión de la Seguridad de la Información. La FISCALÍA GENERAL DE LA NACIÓN mantendrá dentro de su planta de empleados, funcionarios encargados de la seguridad de la información, cuyas funciones estarán caracterizadas y definidas según la necesidad de la Entidad.

Seguridad en la Conexión con Terceros. Es responsabilidad de la Oficina de Informática que todas las conexiones autorizadas de terceros a la red interna de FISCALÍA GENERAL DE LA NACIÓN sean implementadas y monitoreadas desde el punto de vista técnico según las condiciones contractuales establecidas.

Los contratos que incluya el uso de tecnología informática que se suscriban con terceros, cualquiera sea su naturaleza, deberán incluir los acuerdos para cumplir las politicas de seguridad de la Información establecidas por la FISCALÍA GENERAL DE LA NACIÓN.

En los contratos que de manera directa o indirecta transfiera la responsabilidad de la seguridad de la información a un tercero, deben incluir las cláusulas necesarias que de manera explicita establezcan el compromiso por las dos partes, referente a la aplicación de los controles de seguridad requeridos por la FISCALÍA GENERAL DE LA NACIÓN.

Responsabilidad por la información. Cada conjunto de datos tendrá un usuario dueño y responsable, donde se entiende por dueño de la información a la FISCALÍA GENERAL DE LA NACIÓN y el responsable al área donde esta se genera.

Es responsabilidad de la FISCALÍA GENERAL DE LA NACIÓN y en cabeza de la Oficina de Informatica, mantener segura la información suministrada en las plataformas de TIC por las áreas responsables de la información.

5.2. SEGURIDAD DEL RECURSO HUMANO.

Responsabilidades de los usuarios. Todos los servidores de la FISCALÍA GENERAL DE LA NACIÓN, deberán conocer, entender y asumir sus responsabilidades con respecto al cumplimiento de las Políticas de seguridad de la información, así como:

a) El incumplimiento de alguna de las Políticas o Normas estipuladas en este documento que conlleve a un incidente de seguridad, implicará el proceso respectivo por parte de la entidad para establecer la responsabilidad del usuario involucrado.
b) Con la terminación del contrato de trabajo con la FISCALÍA GENERAL DE LA NACIÓN se deberá entregar los activos de información que estén a su cargo al Jefe inmediato.

5.3. SEGURIDAD FÍSICA Y DEL ENTORNO.

Los controles de acceso físico y del entorno están a cargo del Grupo de Seguridad del Cuerpo Técnico de Investigación (CTI), de acuerdo con lo establecido en la Normatividad Física y del Entorno de la FISCALÍA GENERAL DE LA NACIÓN.

5.3.1. Centro de Cómputo.

a) El área responsable debe establecer los mecanismos de seguridad necesarios para la correcta protección de los activos informáticos del Centro de Cómputo, de manera que se mantenga la confidencialidad y seguridad de la información que se procesa.

b) La FISCALÍA GENERAL DE LA NACIÓN debe proporcionar y mantener las condiciones físicas, ambientales y de monitoreo en óptimas condiciones para los centros de cómputo. (inundación, humedad, monitoreo por el CCTV).

5.3.2. Áreas Restringidas.

La FISCALÍA GENERAL DE LA NACIÓN deberá identificar, clasificar y controlar el acceso a los sitios (áreas) que por su actividad deban operar en forma restringida, teniendo en cuenta los adecuados mecanismos de control y registro de acceso.

5.4. GESTIÓN DE ACTIVOS.

5.4.1. Propietario de los activos.

Política *- Todos y cada uno de los equipos informáticos de la Entidad deben ser asignados a un usuario responsable, por lo que es de su competencia la correcta utilización que se haga de los mismos.*

Normatividad:

a) El usuario responsable del activo informático debe velar por una correcta ubicación e instalación de dicho activo, así como las condiciones de funcionamiento.

b) El usuario del activo informático no debe destapar, desmantelar o romper los sellos de los equipos suministrados por la entidad sin previa autorización.

c) El usuario del activo informático no debe trasladar el equipo de cómputo a su cargo sin previa autorización de la **Dirección Administrativa y Financiera y la Oficina de Informática**.

d) El usuario responsable del activo informático no debe conectar al computador ningún elemento sin previa autorización de la **Oficina de informática**.

e) El usuario responsable del activo informático no debe instalar ningún programa sin previa autorización del Jefe Inmediato y de la **Oficina de informática**.

f) En caso de retirar el equipo fuera de la sede de la Entidad el Jefe de la dependencia a la que pertenece el equipo debe enviar un memorando a la Dirección Administrativa y Financiera, de igual forma a la Oficina de Informática, informando de tal situación y solicitando la autorización respectiva.

5.4.2. Uso aceptable de los activos.

Política - Las herramientas informáticas que la Entidad asigna a los usuarios con ocasión a sus funciones, son de su absoluta responsabilidad, tanto el uso adecuado, como su tenencia y custodia.

Normatividad:

a) Los usuarios de la FISCALÍA GENERAL DE LA NACIÓN están obligados a utilizar las herramientas informáticas que la Entidad les proporciona para el desarrollo de su trabajo. Cuando dicho servidor considere que no requiere del recurso asignado para desempeñar su labor, deberá devolverlo al Almacén de la Entidad, con el respectivo concepto técnico previo de la Oficina de Informática.

b) El recurso informático que se encuentre fuera de servicio por daños en hardware y/o software, debe ser reportado a la Oficina de Informática o en su defecto a los Analistas de Sistemas de cada Seccional, registrando el respectivo incidente en la mesa ayuda.

c) Se prohíbe la instalación y uso de herramientas que permitan el acceso a información y servicios no autorizados (uso de sniffers, proxys, escritorios remotos, etc.).

d) El usuario no debe modificar la configuración y características de un PC. Está prohibido instalar, desinstalar o bajar software de Internet, a menos que se tenga la debida autorización de la Oficina de Informática.

e) El computador que la Entidad asigna al servidor o a un tercero debe contar con un sistema operativo y ofimática respectivamente licenciados, y un aplicativo para eliminar y prevenir la instalación de software malicioso (antimalware), activado y con actualizaciones diarias.

f) Para efectos de auditoria, es necesario que la fecha y hora del computador esté sincronizada con la hora legal de Colombia, por lo que se prohíbe su modificación.

g) El usuario empleará exclusivamente los recursos informáticos para desarrollar su trabajo en función del cargo que desempeña. No para fines políticos, religiosos, comerciales o de diversión personal.

h) Se prohíbe la copia, reproducción o almacenamiento de videos, juegos, películas, fotos, música en los computadores arrendados o propios de la Fiscalía, a menos que sean materia de investigación o en general que sirva de apoyo para la gestión de la entidad.

i) El mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad, es responsabilidad de las áreas encargadas de la plataforma TIC o a los que estos deleguen para tal fin, por lo que se prohíbe que los equipos sean manipulados por personas que no tengan dicha función. Se excluyen los investigadores del CTI, sí el equipo de cómputo es materia de investigación.

5.4.3. Uso aceptable de los servicios informáticos.

5.4.3.1. Correo Electrónico Institucional

Política *- Todo servidor o funcionario de la Entidad que posea un usuario o una cuenta de red, puede contar con servicio de correo electrónico institucional suministrado por la Fiscalía General de la Nación.*

Normatividad:

a) La dirección de correo electrónico institucional deberá crearse de la siguiente manera: nombre.apellido@fiscalia.gov.co.

En donde nombre.apellido corresponde al nombre y apellido del titular de la cuenta y fiscalia.gov.co, es el dominio registrado por la FISCALÍA GENERAL DE LA NACIÓN.

En caso que por necesidades del servicio se deba crear una cuenta institucional se debe establecer su responsable y crearse de la siguiente manera: nombre unidad.ciudad@fiscalia.gov.co.

b) Los mensajes de correo pueden considerarse como elementos probatorios de acuerdo con la Ley 527/99 por medio de la cual se define y reglamenta el uso de mensajes de datos, del Comercio Electrónico y firmas digitales.

c) El servidor o funcionario de la Entidad deberá diligenciar el formato correspondiente, definido en el SGI, para que le sea asignada una cuenta de correo electrónico institucional, en el cual se compromete a mantener la confidencialidad de su contraseña de acceso la cual es personal e intransferible

d) El usuario debe enviar y recibir la información de la Entidad inherente al desarrollo de su labor a través de la cuenta de correo electrónico institucional que le fue asignada y no a través de cuentas de correo personales, públicas o comerciales. Así mismo debe incluir en todos los mensajes la información correspondiente al nombre, cargo, área, seccional, dependencia, grupo y teléfono.

e) En caso de existir sospecha de que su seguridad ha sido vulnerada podrá solicitar el cambio de su usuario y contraseña, con la respectiva sustentación diligenciando el formato correspondiente.

f) Es responsabilidad del usuario leer, depurar y respaldar el contenido de su respectivo buzón de correo, dado que éste tiene capacidad limitada de almacenamiento.

g) Las circulares, memorandos y comunicaciones electrónicas oficiales en general, deben ser enviadas desde los buzones institucionales de la dependencia que los emite, con visto bueno y autorización del Jefe de la misma.

h) Todas las personas que tengan acceso al servicio de correo electrónico institucional de la Fiscalía, deben estar identificadas plenamente como: Servidores Públicos de la FISCALÍA GENERAL DE LA NACIÓN, Contratistas autorizados, judicantes, estudiantes en pasantías y funcionarios de otras entidades autorizados por Ley, por convenio, contrato u orden de servicio. Por lo tanto, no se permite el acceso al servicio de correo sin la previa solicitud emitida por los responsables de los convenios, supervisores de los contratos, prestaciones del servicio y/o jefes de las dependencias donde laboran dichas personas.

i) La responsabilidad del contenido de los mensajes de correo será del usuario remitente.

j) La información de carácter confidencial que se transmita a través del servicio de correo electrónico, debe ser emitida con los medios de seguridad que disponga (como por ejemplo un archivo anexo elaborado en cualquier herramienta de Office, deberá ir con alguna clave de acceso de seguridad).

Prohibiciones en el uso del correo electrónico institucional:

a) No se debe utilizar ningún tipo de procedimiento o herramienta que permita ocultar o tergiversar el nombre del remitente.

b) No se debe utilizar ningún tipo de procedimiento o herramienta que afecte el normal desempeño de otras máquinas, tal como el uso del servicio de correo electrónico institucional para el envío de software malicioso (virus, troyanos, etc.) y el envío de mensajes con información no solicitada, a todos los usuarios de la red (spam).

c) No se debe utilizar el correo institucional para el envío información no autorizada, tal como propaganda comercial, política o religiosa, envío de material amenazador, difamatorio, calumnioso, racista, pornográfico y en general ilegal.

d) No se debe realizar ninguna actividad que vaya en contra de las normas disciplinarias de la Entidad, enmarcadas en la Ley 734 de 2002 "Código Único Disciplinario", Ley 938 del 2004 "Estructura de la Fiscalía General de la Nación" Art. 78 y Ley 594 de 2000 Título I, Art. 3 "Ley General de Archivos".

e) No suplantar la cuenta de correo electrónico de otro usuario.

f) No se debe transmitir información que se considere de uso exclusivo y/o confidencial sin la autorización del responsable de la información y con los mecanismos adecuados para su transmisión.

g) No se debe utilizar lenguaje inapropiado y ofensivo.

5.4.3.2. Uso del servicio de Internet proporcionado por la entidad.

Política *- Todo usuario con acceso a Internet tiene un perfil que determina los sitios a los cuales puede acceder como apoyo a la gestión que realiza en la entidad. Este perfil no podrá ser modificado, salvo con autorización del jefe inmediato y el procedimiento definido.*

Normatividad:

a) El servicio de Internet en la entidad deberá utilizarse exclusivamente como apoyo a las actividades laborales del funcionario.

b) Se autoriza el uso de los recursos informáticos para capacitación a distancia, siempre y cuando este enmarcado en proyectos o convenios que desarrolle la Entidad y debidamente autorizado por el Jefe inmediato.

c) Se prohíbe descargar e instalar software desde Internet que no estó debidamente licenciado y sin autorización de la Oficina de Informática.

d) Se restringe al interior de la entidad el uso de los servicios de mensajeria instantánea tales como News, Real Audio, Netmeeting, Skype, Messenger y redes sociales tales como Facebook y Twitter entre otras redes sociales, constituyen un riesgo de seguridad informática, debido a los ataques y la información que se filtra a través de ellos. Si el usuario necesita utilizar alguno de estos servicios por razones laborales, deberá ser solicitado mediante diligenciamiento del formato correspondiente, definido en el SGI y autorizado por el Jefe de la dependencia, asumiendo el riesgo en el acceso a sitios no seguros de Internet.

e) La FISCALÍA GENERAL DE LA NACIÓN se reserva el derecho de restringir el acceso a sitios no seguros y que no sean necesarios para apoyar el desarrollo de las actividades laborales.

f) El uso del servicio no autorizado de Internet será responsabilidad exclusiva del usuario que tenga acceso a este servicio, y asumirá las sanciones disciplinarias pertinentes a que haya lugar.

g) El Jefe de la Dependencia será el responsable de autorizar o desautorizar el acceso a Internet del personal a su cargo.

h) La FISCALÍA GENERAL DE LA NACIÓN, en cabeza de la Oficina de informática, se reserva el derecho de monitorear, restringir, bloquear y analizar permanentemente el uso de los servicios informáticos de la Entidad, mediante herramientas técnicas adquiridas para tal fin.

i) La Oficina de Informática enviará informes aleatorios o por solicitud expresa de los Jefes de las Dependencias acerca del uso del servicio de Internet, con el fin de optimizar este recurso.

5.5. CONTROL DE ACCESO.

Política – *Todas las personas que tengan acceso a los recursos informáticos de la Entidad, deben estar identificadas plenamente.*

Normatividad:

5.5.1. Acceso a Áreas Críticas:

a) El control de acceso se llevará acabo de acuerdo a las normas y procedimientos establecidos por la FISCALÍA GENERAL DE LA NACIÓN, en concordancia con la política de seguridad, efectuando el registro permanente de ingresos y salidas, sin excepción.

b) Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso estará sujeto a las condiciones y directrices que para tal fin determine el Fiscal General de la Nación.

5.5.2. Control de acceso al equipo de cómputo:

a) Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

b) Las áreas donde se tiene equipo de propósito general cuya misión es crítica deberán cumplir con las normas de seguridad que la Oficina de Informática emita.

c) Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán cumplir las normas que establezca la Oficina de Informática.

d) Los accesos a las áreas críticas de cómputo deberán ser clasificados de acuerdo a las normas que dicte la Oficina de Informática.

e) Para el control de impresión el servidor de la FISCALÍA GENERAL DE LA NACIÓN, deberá contar con una contraseña de acceso en las impresoras de red para iniciar el proceso de impresión.

5.5.3. Control de acceso a la red de datos:

a) La Oficina de Informática es responsable de monitorear el acceso de los usuarios a los recursos informáticos.

b) La Oficina de Informática es la responsable de difundir las políticas para el uso de la red y de velar por su cumplimiento.

c) Dado el carácter unipersonal del acceso a la Red de la FISCALÍA GENERAL DE LA NACIÓN, la Oficina de Informática verificará el uso responsable, de acuerdo al reglamento para el uso de la red.

d) El acceso a equipos especializados de cómputo (servidores, enrutadores, bases de datos, equipos activos de red, etc.) conectado a la red es administrado por la Oficina de Informática o a quien esta asigne.

e) Todo equipo de cómputo que esté o sea conectado a la Red de la FISCALÍA GENERAL DE LA NACIÓN, o aquellas que en forma autónoma se tengan y que sean propiedad de la entidad, debe de sujetarse a las políticas de acceso que emite la Oficina de Informática.

5.5.4. Control de acceso remoto:

a) La Oficina de Informática es la responsable de proporcionar el servicio de acceso remoto de acuerdo con las políticas de acceso a los recursos informáticos disponibles.

b) Para el caso especial de requerirse acceso por parte de terceros a los recursos de equipos de cómputo servidores, deberá ser autorizado por las áreas responsables y la Oficina de Informática.

c) El usuario de estos servicios deberá sujetarse las políticas de uso de la Red de la FISCALÍA GENERAL DE LA NACIÓN.

5.5.5. Acceso a los sistemas administrativos y misionales:

a) Tendrá acceso a los sistemas administrativos solo el personal de la FISCALÍA GENERAL DE LA NACIÓN o la persona que tenga la autorización por parte de la Oficina de Informática.

b) El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

c) Se prohíbe el acceso de personal no autorizado a los servidores de bases de datos, excepto para el personal autorizado de la Oficina de Informática.

d) El servidor o funcionario de la Entidad deberá diligenciar el formato correspondiente para que le sea asignada una cuenta de acceso a los sistemas administrativos y misionales.

e) El usuario se compromete a mantener la confidencialidad de su contraseña de acceso y de los datos consultados de carácter reservado, privado o confidencial.

5.6. GESTIÓN DE ACCESO DE USUARIOS.

5.6.1. Registro de Usuarios.

Política – Todo servidor de la Entidad o tercero autorizado deberá tener un "nombre de Usuario" (user name) y una contraseña (password) para tener acceso a la red, a las aplicaciones y a los servicios informáticos de la FISCALÍA GENERAL DE LA NACIÓN

Normatividad:

a) Las cuentas de usuario serán creadas de acuerdo con la solicitud diligenciada mediante el formato correspondiente, establecido para este fin por la Oficina de Informática, en el marco del proceso de Gestión de Calidad.

b) Todo "nombre de usuario" debe estar asociado a un perfil asignado, que determine los permisos y restricciones de acuerdo con sus funciones. Este perfil no podrá ser modificado, salvo autorización del jefe inmediato y diligenciado mediante el formato establecido y definido en el SGI.

c) El "nombre de usuario" debe ser único e intransferible, es decir que está prohibido el acceso a los recursos informáticos de la Entidad por medio de un "nombre de usuario" compartido o que no se le haya asignado.

d) Los usuarios son responsables de todas las actividades que involucren el uso de su "nombre de usuario".

e) Solo se aceptan solicitudes de acceso a servicios informáticos de la Entidad, con la debida autorización del Jefe de la Dependencia y aprobación del administrador de la información del servicio informático.

5.6.2. Gestión de contraseñas para usuarios.

Política - Para gestionar correctamente la seguridad de las contraseñas, los usuarios deben tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Normatividad:

a) Junto con su nombre de usuario el funcionario recibirá una contraseña o clave de acceso, la cual debe cambiar en el primer ingreso, por cuanto es su responsabilidad la administración y único conocimiento sobre la misma.

b) La contraseña debe tener una longitud mínima de ocho (8) caracteres alfanuméricos, diferentes de nombres propios, nombres de animales, ciudades, es decir ninguna palabra que pueda identificarse fácilmente.

c) Por seguridad, las contraseñas tienen una caducidad de sesenta (60) días, al cabo de los cuales, el sistema solicitará su cambio. Este cambio es de carácter obligatorio y no se podrá utilizar contraseñas empleadas con anterioridad.

d) Los usuarios de red se bloquearan automáticamente después de tres (3) intentos no exitosos al digitar su contraseña, al cabo de cinco (5) minutos, el usuario será habilitado se automáticamente o también podrá solicitar su desbloqueo a los administradores del servicio, previa comprobación de la identidad del solicitante.

e) Si sospecha que su usuario y contraseña de red está siendo utilizadas por otra persona, solicite inmediatamente el cambio de contraseña a la Oficina de Informática (Centro de Cómputo) diligenciando el formato correspondiente, definido en el SGI.

f) Se prohíbe el uso de contraseña compartida. Las contraseñas nunca deben ser compartidas o reveladas a otras personas diferentes al usuario autorizado. El hacerlo expone al usuario a enfrentar la responsabilidad por acciones que otros puedan llevar a cabo con dicha contraseña.

g) Las contraseñas nunca serán modificadas vía línea telefónica.

5.6.3. Activación, Inactivación, bloqueo y cancelación de cuentas de Usuario.

Política *- Las cuentas de usuario tendrán un tiempo límite para su activación e inactivación y podrán ser monitoreadas para determinar su bloqueo o cancelación por parte de la Oficina de Informática.*

Normatividad:

a) Las cuentas de usuario que presenten una inactividad superior a 90 días serán desactivadas temporalmente y su restablecimiento solo se dará con la correspondiente justificación del usuario asignado mediante solicitud expresa del jefe de la dependencia a través del correspondiente formato.

b) Las cuentas que en un término de 90 días posteriores a la desactivación no hayan sido reportadas para su activación, serán eliminadas definitivamente, salvo en aquellos casos que por situaciones administrativas ameriten la disponibilidad de la cuenta activa.

c) En todos los casos en que se establezca el uso indebido de la cuenta se procederá al bloqueo temporal de la misma, conforme a los procedimientos y sanciones disciplinarias establecidas.

d) Son causales de bloqueo y/o cancelación de cuentas las novedades administrativas de retiro, traslado o cambio de funciones de los usuarios.

5.6.4. Control de acceso a las redes.

Política *- El servicio de acceso a red será proporcionado a todo usuario autorizado que cuente con un equipo de cómputo autorizado por la entidad y que requiera hacer uso de la red.*

Normatividad:

a) La Oficina de Informática es la responsable de monitorear el acceso lógico y físico a las redes a través del grupo de comunicaciones:

- *Conectividad a la red local (LAN) con nodos alámbricos e inalámbricos*
- *Acceso a Internet*
- *Acceso a Servicio ofrecidos por el OINF, siendo éstos:*
  - *Correo electrónico.*
  - *Sistemas administrativos, misionales y de apoyo.*

b) Los servidores de la Entidad y terceros deberán acatar las normas, procedimiento y controles establecidos para el acceso a los recursos de red ofrecidos.

5.6.5. Controles sobre el uso de la red.

Política - Se prohíbe la utilización de los recursos de red por parte de los usuarios para:

Normatividad:

a) Acceder a servicios locales o remotos a los que el usuario no tenga autorización explícita o intentar violar la seguridad de acceso a cualquier equipo computacional o de red.

b) Vulnerar los derechos de propiedad intelectual de terceras partes a través de los servicios de red.

c) Adelantar acciones de corrupción, destrucción de datos o cualquier actividad que pueda impedir el acceso legítimo a los datos; esto incluye la carga de virus, gusanos o cualquier software dañino en cualquier sistema de cómputo conectado a la red.

d) Hacer transmisión de amenazas, material obsceno, pornografía o de hostigamiento.

e) Usar la red para acceder a páginas catalogadas como ocio y juegos.

f) Transmitir publicidad ilegal o para actividades con ánimo de lucro.

g) Instalar servicios web, ftp, dhcp, dns, irc, de correo o configurar una dirección IP no autorizada en los dispositivos conectados en red.

h) Usar programas para realizar conexiones entre dos o más puntos de la red o de internet para fines no laborales.

i) Acceder a sitios con contenido o material pornográfico u ofensivo que no esté enmarcado dentro de los procesos de investigación que adelante la Entidad. La persona que sea sorprendida realizando descargas o visitando sitios pornográficos sin ser autorizada, será sancionada conforme al reglamento vigente.

j) Realizar la instalación de equipos a la red institucional sin ser autorizado por la Oficina de Informática.

5.6.5.1. Derechos de los usuarios:

a) Los usuarios tiene derecho a utilizar la red de acuerdo con las políticas establecidas y cumplan con los puntos antes mencionados.

6.6.6. Autenticación de usuarios para conexiones externas de terceros.

Política - La Fiscalía General de la Nación proporcionará a sus usuarios autorizados, tecnologías de acceso remoto seguro, cuya operación será realizada por la Oficina de Informática.

Normatividad:

a) Toda solicitud de acceso a los sistemas de información de la FISCALÍA GENERAL DE LA NACIÓN por parte de terceros, debe estar respaldada por convenio, contrato o acuerdo, y avalada técnicamente por la Oficina de Informática.

b) La conexión de un computador remoto a un computador específico que se encuentre en la red interna de la FISCALÍA GENERAL DE LA NACIÓN debe hacerse mediante un sistema seguro con Encripción y autenticación, a través de una Red Privada Virtual (VPN).

c) La autenticación de acceso remoto será llevado a cabo mediante la utilización de un esquema de llaves publicas/privadas, acompañadas con el uso de una contraseña fuerte. (Ver 5.6.2. Gestión de contraseñas para usuarios).

d) Las credenciales de identificación serán entregadas por la Fiscalía a los usuarios externos luego de diligenciar el formato correspondiente ante la Oficina de Informática que incluye el compromiso de confidencialidad y cumplimiento de las políticas establecidas por la Entidad. Dichas credenciales serán únicas e intransferibles.

e) El usuario se compromete a finalizar cada sesión de VPN, conforme a las instrucciones dadas por la Oficina de Informática.

5.6.7. Trabajo Remoto.

Política - *Los usuarios de la FISCALÍA GENERAL DE LA NACIÓN que requieran desarrollar su labor desde una ubicación diferente a su puesto de trabajo, podrán hacerlo mediante las herramientas informáticas dispuestas para tal fin, previa autorización del jefe de la dependencia donde labora.*

Normatividad:

a) El servidor o funcionario de la Entidad deberá diligenciar el formato correspondiente, definido en el SGI, para que le sea asignada una cuenta de trabajo remoto, en el cual se compromete a mantener la confidencialidad de su contraseña de acceso la cual es personal e intransferible.

b) Por seguridad, las cuentas de trabajo remoto tienen una caducidad de treinta (30) días, por inactividad. Para reactivar la cuenta se debe diligenciar el formato correspondiente.

c) Para el acceso, el usuario debe tener instalado y licenciado en el computador remoto tanto el sistema operativo como un programa de protección contra software malicioso (Firewall, antivirus, antispyware, antimalware) con actualizaciones diarias.

d) El computador utilizado para acceder a la red de la FISCALÍA GENERAL DE LA NACIÓN no debe conectarse al mismo tiempo a otro tipo de red.

e) Para el caso de conexión con redes de otras entidades los usuarios habilitados para ingresar a la red de la FISCALÍA GENERAL DE LA NACIÓN deben cumplir con las políticas de seguridad establecidas por ésta y lo contemplado al respecto en convenio, contrato o acuerdo.

f) Los equipos informáticos (Computadores, enrutadores, switches) que se utilicen en la conexión remota deben tener actualizado su sistema operativo y tener protegido el acceso a su configuración mediante una contraseña segura.

g) El usuario podrá ingresar única y exclusivamente a los servicios autorizados por la FISCALÍA GENERAL DE LA NACIÓN.

h) Si la información a la que tiene acceso el usuario es de carácter confidencial o sujeto a la reserva legal, este se compromete a seguir manteniendo su condición.

5.6.8. Computación y Comunicaciones Móviles.

Política *Los usuarios de la FISCALÍA GENERAL DE LA NACIÓN que requieran desarrollar su labor mediante computadores portátiles y dispositivos móviles que sean propiedad de la entidad a través de las herramientas informáticas dispuestas para tal fin, deberán contar con la autorización del jefe de dependencia donde labora y la Oficina de Informática.*

Normatividad:

a) El usuario debe tener instalado y actualizado en el computador portátil o dispositivo móvil un programa de protección contra software malicioso (Firewall, antivirus, antispyware, antimalware) con actualizaciones diarias.

b) Todos los dispositivos personales de información, como computadores portátiles de propiedad de los funcionarios o asistentes digitales personales (BlackBerry, Palm OS, Symbian OS, Windows Mobile, Android, iPhone, Ipad etc.), no están autorizados para interactuar con los sistemas de comunicaciones de la FISCALÍA GENERAL DE LA NACIÓN. En el caso de requerirse por necesidades del servicio este debe ser autorizado por el Fiscal General de la Nación o al que este delegue.

c) Se desarrollarán procedimientos adecuados para estos tipos de dispositivos, que abarquen la protección necesaria para el acceso a los sistemas de información y servicios de la entidad mediante técnicas criptográficas en la transmisión de información clasificada.

5.7. PROPIEDAD Y PROCESAMIENTO DE LA INFORMACIÓN.

Política - *Toda información generada por los servidores públicos de la FISCALÍA GENERAL DE LA NACIÓN, con ocasión a sus funciones es de propiedad de la Fiscalía General de la Nación.*

Normatividad:

a) Todos los sitios o páginas WEB que la Fiscalía publique deberán estar incorporadas al dominio fiscalia.gov.co, salvo autorización escrita de la Oficina de Informática. Para su diseño y publicación se seguirán los lineamientos determinados por la Oficina de Prensa.

b) El usuario es responsable de la custodia, integridad y confidencialidad de la información oficial contenida en los recursos informáticos (PC, USB, Discos, cintas) que le han sido asignados por la Entidad. Así como las copias de seguridad para garantizar la disponibilidad de la información almacenada en dichos recursos.

c) Se prohíbe publicar en información que atente contra los derechos fundamentales de las personas naturales y jurídicas.

d) Se prohíbe publicar opiniones personales como si fueran propias de la Entidad.

e) No se permite publicar o dar a conocer información de propiedad de la Entidad que esté sujeta a la reserva legal o de carácter confidencial.

f) Se prohíbe la instalación de equipos de cómputo, servidores de aplicaciones, servicios Internet y servicios de red en general, sin la debida autorización de la Oficina de Informática.

g) Los Jefes de dependencia, sección, o área, son los primeros responsables de la integridad y respaldo de la información inherente de la dependencia a su cargo. Dicha labor de respaldo podrá adelantarla con la asesoría técnica de la Oficina de Informática.

5.8. GESTIÓN DE LA SEGURIDAD DE LAS REDES.

Política - *Los usuarios y administradores de las redes de la Fiscalía General de la Nación deberán hacer uso adecuado de los recursos y servicios soportados en este tipo de plataformas.*

Normatividad:

a) Se Prohíbe distribuir archivos que contengan virus, troyanos, gusanos, spyware y en general todo tipo de software malicioso, con el fin de atentar contra la confidencialidad, integridad y disponibilidad de los recursos informáticos.

b) Se prohíbe el uso de la red de computadores de la Entidad para obtener acceso no autorizado a información o servicios en otros computadores.

c) Se prohíbe el uso de los recursos informáticos para la consulta o envío de material pornográfico, racista u ofensivo, a menos que haga parte de una investigación.

d) Se prohíbe la instalación y uso de equipos de comunicaciones (módems, sistemas inalámbricos) que permitan conectar la red de computadores de la Fiscalía con otras redes externas, sin la debida autorización por parte del Fiscal General de la Nación o a quien este delegue.

e) El ingreso de equipos portátiles de procesamiento y/o almacenamiento (computadores portátiles, celulares, Mp4, USB, etc.) debe ser autorizado por el personal de Seguridad de la respectiva sede de la Fiscalía y la responsabilidad del uso será asumida por el funcionario que autorizo el ingreso.

5.8.1. Uso de los bienes y servicios informáticos por terceros.

Política *– Para la utilización de los recursos informáticos por parte de terceros que se encuentren laborando al interior de la Entidad, deberán cumplir con las Normas y Políticas de Seguridad Informática de la FISCALÍA GENERAL DE LA NACIÓN.*

Normatividad:

a) El Tercero deberá solicitar previamente el permiso de ingreso a las instalaciones de la Fiscalía de los equipos necesarios para su trabajo con el visto bueno de un servidor de la FISCALÍA GENERAL DE LA NACIÓN que avale la necesidad de uso.

b) El Tercero debe tener debidamente licenciado todo el software instalado en su computador.

c) El Tercero debe tener instalado y licenciado en su computador un programa de protección contra software malicioso (antivirus, antispyware, antimalware) con actualizaciones diarias.

d) El Tercero, mientras esté en las instalaciones de la Fiscalía, no podrá utilizar medios de comunicación sin previa autorización.

e) Los equipos informáticos (computadores y equipos de comunicaciones) que utilice el Tercero durante su estadía en las instalaciones de la Fiscalía deben tener actualizado su sistema operativo y tener protegido el acceso a su configuración mediante una contraseña segura.

f) El Tercero podrá ingresar única y exclusivamente a los servicios autorizados por la Fiscalía.

g) Si la información a la que tiene acceso el Tercero es de carácter confidencial o sujeto a la reserva legal, este se compromete a seguir manteniendo su condición.

La Fiscalía se reserva el derecho de monitorear el buen uso que se dé a los servicios concedidos y de renovarlos o suspenderlos, de acuerdo con el cumplimiento que se haga de la normatividad establecida para una correcta utilización de los recursos informáticos de la Entidad.

5.8.2. Responsabilidades y funciones.

Es necesario que cada uno de los servidores de la Entidad como parte activa en la gestión de seguridad informática, conozca y de cumplimiento a las responsabilidades y funciones establecidas para tal fin, por lo que el Fiscal General de la Nación como actor primordial en el logro de la misión institucional prestará el apoyo para el diseño, implementación, puesta en funcionamiento, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información de la Entidad, mediante el establecimiento de una política de seguridad informática del SGSI que incluya la formulación de los objetivos, planes, funciones y responsabilidades en materia de seguridad informática.

ARTICULO SEXTO. – RESPONSABILIDADES Y FUNCIONES.

1. Propietarios de la Información:

a. Son responsables de clasificar y documentar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.

b. Mantener actualizada la clasificación de la información

c. Definir quiénes deben tener asignado un usuario y los permisos de acceso a la información de acuerdo a sus funciones y competencia.

2. Usuarios de los activos informáticos.

Los servidores de la Entidad y principalmente los Directores Nacionales, Directores Seccionales, Jefes de Oficina, Jefes de División, Jefes de Sección, Jefes de Unidades y en general todos aquellos servidores y funcionarios de la Entidad con personal a cargo, tienen la responsabilidad de:

a. *Conocer, divulgar, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.*

3. La Oficina de Informática.

Es responsable de asesorar al Fiscal General de la Nación en el establecimiento de una política de seguridad informática y apoyar el desarrollo de las siguientes funciones:

a. *Revisar y proponer la Política de Seguridad Informática para aprobación del Fiscal General de la Nación y así como las funciones generales en materia de seguridad informática.*

b. *Apoyar el establecimiento e implementación de una metodología de análisis, evaluación y gestión de riesgos de activos informáticos.*

c. *Monitorear y evaluar los cambios significativos en los riesgos que afectan a los activos informáticos frente a las amenazas más importantes de acuerdo con los criterios y niveles para la aceptación de riesgos a los que se ven abocados los activos informáticos de la Entidad.*

d. *Apoyar la revisión y actualización periódica de la Política de Seguridad Informática, teniendo como marco los siguientes aspectos:*

- *Identificación y documentación de nuevos riesgos que afecten los activos informáticos provenientes de amenazas internas y externas.*
- *Evaluación de los Incidentes relativos a la seguridad informática en la Entidad producto del monitoreo y análisis de los mismos.*
- *Recopilación de iniciativas provenientes de las dependencias de la FISCALÍA GENERAL DE LA NACIÓN, con el fin de mejorar la seguridad de la información.*
- *Evaluación de los avances tecnológicos relacionados con la seguridad informática y la viabilidad de implementación en la FISCALÍA GENERAL DE LA NACIÓN, con el fin de mejorar la seguridad de la información.*

e. *Apoyar la implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información de la Entidad, así como los objetivos y planes que se formulen dentro de este ámbito.*

f. Formular soluciones tecnológicas para incrementar la seguridad informática, de acuerdo a las competencias y responsabilidades identificadas en la Entidad.

g. Formular metodologías y procesos específicos relativos a seguridad informática.

h. Apoyar el desarrollo de la cultura organizacional en aspectos de seguridad informática como parte del proceso de planificación de la información.

i. Apoyar la formulación y seguimiento de planes de divulgación de la importancia de cumplir los objetivos de seguridad de la información a través de la Escuela de Estudios de la FISCALÍA GENERAL DE LA NACIÓN.

j. Evaluar y coordinar la implementación de controles específicos de seguridad informática para nuevos sistemas o servicios.

k. Apoyar la difusión de la seguridad informática dentro de la Entidad.

l. Apoyar los planes de recuperación y continuidad de servicios informáticos de la Entidad.

m. Apoyar las acciones tendientes a impulsar la implementación y cumplimiento de la Política de seguridad Informática.

n. Apoyar la realización de las funciones relativas a la seguridad informática de la Entidad, lo cual incluye lo relacionado con la supervisión de todos los aspectos inherentes a los temas tratados en la Política de Seguridad Informática.

ñ. Identificar y gestionar los requerimientos de seguridad informática para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Entidad.

o. Realizar las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología apropiada de ciclo de vida y que contemple las medidas de seguridad en todas sus fases.

p. La ejecución de los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas de información y de los recursos de tecnología de la Entidad.

q. Coordinar, planear y promover todas aquellas actividades que tengan como fin el mantener la disponibilidad, confidencialidad e integridad de todos los activos informáticos de la Entidad, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

r. Adelantar los procesos de selección de herramientas y proveedores en materia de seguridad informática.

s. Definir la estructura de restricciones y excepciones de acceso a la información de todo el personal, de acuerdo a las pautas de la política de seguridad y a las necesidades de acceso de los usuarios en conformidad con las funciones que desempeñan.

t. Identificar los activos informáticos más valiosos de la institución.

u. Promover la difusión y actualización permanente de las Políticas de Seguridad Informática de la institución, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.

v. Promover la aplicación de auditorías enfocadas a la seguridad informática.

4. **La Oficina de Personal.**

En cumplimiento a la Política de seguridad Informática debe asesorar al Fiscal General de la Nación en:

a. *Reportar las novedades de personal a la Oficina de Informática: vacaciones, permisos, retiros, traslados, comisiones, para que se tomen las acciones necesarias sobre los sistemas de información.*

b. *Notificar a todo el personal que ingresa a la Institución, de sus obligaciones respecto del cumplimiento de la Política de Seguridad informática.*

5. **La Escuela de Estudios e Investigaciones Criminalísticas y Ciencias Forenses.**

En cumplimiento a la Política de seguridad Informática debe asesorar al Fiscal General de la Nación en:

a. *Realizar las tareas de capacitación continua en materia de seguridad informática, a todos los servidores y funcionarios de la Fiscalía.*

b. *Divulgar e informar a los servidores y funcionarios de la Fiscalía los cambios o actualizaciones que se produzcan en la Políticas de Seguridad Informática.*

6. **La Oficina Jurídica.**

En cumplimiento a la Política de seguridad Informática se debe encargar de asesorar al Fiscal General de la Nación en:

a. *Asesorar en materia legal de los cambios o ajustes que se deban realizar a las Políticas de Seguridad Informática de la Entidad.*

7. **La Oficina de Control Interno.**

En cumplimiento de la Política de seguridad Informática se debe encargar de asesorar al Fiscal General de la Nación en:

a. *Realizar auditorías periódicas sobre la operación de los sistemas de información por parte de los usuarios y el uso adecuado de los recursos informáticos de la Entidad.*

b. Informar sobre el cumplimiento por parte de los usuarios de los estándares, la reglamentación y las medidas de seguridad informática establecidas por esta Política, así como de las normas, procedimientos y prácticas que de ella surjan.

ARTÍCULO SEPTIMO.- La presente resolución rige a partir de la fecha de su publicación.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 06 NOV. 2013

EDUARDO MONTEALEGRE LYNETT
Fiscal General de la Nación

FUNCIONARIO	NOMBRE	FIRMA	FECHA
Vo. Bo.	Carlos Ariel Useda Gómez, Jefe Oficina de Informática		14-10-13
Proyectó:	Oscar Leonardo Perez Casilmas, Área Seguridad Informática		17-10-13
Revisó:	Alexandra Katherine Manzano Guerrero, Jefe Oficina Jurídica		24-09-13
Aprobó:	Isadora Fernández Posada, Jefe Oficina de Planeación		16-10-13

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma.