| | | | | |
|---|---|---|---|---|
| ALCALDÍA MAYOR DE BOGOTÁ D.C. GOBIERNO, SEGURIDAD Y CONVIVENCIA Fondo de Vigilancia y Seguridad | **Proceso:** | GESTION DE LAS TIC | **Código:** | GTI-PO-01 |
| | **Procedimiento:** | ADMINISTRACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA | **Versión:** | 1 |
| | | | **Fecha Aprobación:** | 07/05/2015 |
| | **Documento:** | POLITICAS Y ESTANDARES DE SEGURIDAD DE LA INFORMACIÓN | **Acto Administrativo:** | Resolución 421 de 2009 |
| | | | **Páginas:** | 1 de 19 |

| **Firma de Autorizaciones** | | | | | |
|---|---|---|---|---|---|
| **ELABORÓ** | | **REVISÓ** | | **APROBÓ** | |
| **Nombre(s):** | Milton Yair Moreno Zamudio | **Nombre(s):** | Edgar Raúl Quintero Rojas | **Nombre(s):** | Ricardo Ramirez Moreno |
| **Firma (s):** | | **Firma (s):** | | **Firma (s):** | |
| **Cargo (s):** | Contratista | **Cargo (s):** | Director TIC | **Cargo (s):** | Subgerente Técnico |

| **Control de Cambios** | | |
|---|---|---|
| **Fecha** | **Versión** | **Descripción** |
| 7/5/2015 | 1 | Se adelanta la creación del documento con el objeto de regular las actividades al interior de la entidad en cuanto a la Seguridad de la Información. |

# Contenido

## 1. INTRODUCCION

Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros computadores y de nuestras organizaciones. El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves consecuencias.

Una de las posibles secuelas de una intrusión es la pérdida de datos de carácter reservado o restringido. Y el robo de información sensible y confidencial.

Con la constante evolución de las Tecnologías de la Información y las comunicaciones, es fundamental definir los recursos para obtener seguridad en los sistemas de información.

Las políticas de seguridad informática diseñan las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

**CONFIDENCIALIDAD**: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios,

computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

**INTEGRIDAD**: Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

**DISPONIBILIDAD**: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

El presente documento tiene por objeto establecer las medidas de índole técnico y de organización, necesarias para garantizar la seguridad de las tecnologías de información y las comunicaciones (equipos de cómputo, sistemas de información, redes (Voz y Datos)) del Fondo de Vigilancia y Seguridad de Bogotá.

## 2. DESARROLLO GENERAL

### 2.1. Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC, garantizando la integridad, confidencialidad y confiabilidad de la información generada, administrada y consultada por el Fondo de Vigilancia y Seguridad, así como el uso de los bienes informáticos de hardware, software y comunicaciones.

### 2.2. Evaluación de las Políticas

El presente documento de políticas y estándares deberá ser revisado y actualizado a medida que los procesos y procedimientos se consoliden y aumenten su nivel de madurez.

### 2.3. Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC) en la Entidad.

### 2.4. Responsabilidad de la aplicación de las Políticas

El personal de la mesa de Ayuda y el administrador del sistema de la Dirección de TIC tienen la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas y estándares de seguridad.

## 3. CONFIDENCIALIDAD y CUMPLIMIENTO

**POLÍTICA**: Toda persona que ingresa como usuario nuevo al Fondo de Vigilancia y Seguridad, para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática.

Todas las actividades que realicen los usuarios, funcionarios y contratistas en la infraestructura Tecnología de Información y Comunicaciones (TIC) del Fondo de Vigilancia y Seguridad serán registradas y podrán ser objeto de auditoria.

### 3.1. Usuarios Nuevos

Todo el personal que ingrese a prestar sus servicios de planta o contratista a la Institución, deberá ser notificado a la Dirección de TIC para asignarle los derechos correspondientes en caso de requerirse (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo). De igual manera a la finalización del contrato o en caso de retiro, se deberá nuevamente informar para anular y cancelar los derechos otorgados como usuario informático.

### 3.2. Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos, cumplir las Políticas y Estándares de Seguridad Informática establecidas en el presente Documento.

### 3.3. Capacitación en seguridad informática

Todo servidor o funcionario nuevo en el Fondo de Vigilancia y Seguridad deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

### 3.4. Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial del Fondo de Vigilancia y Seguridad o que se le declare culpable de un delito informático. Los funcionarios, contratistas o usuarios de la Plataforma tecnológica que incumplan con las políticas y estándares descritos en el presente documento serán objeto de investigación disciplinaria o penal de acuerdo a la normatividad vigente.




Carrera 7 No. 32 – 12 Edificio
Centro Comercial San Martín
Pisos 33 a 36 Bogotá D.C.
Colombia
Código postal: 111711

## 4. SEGURIDAD FISICA Y DE ACCESO

### 4.1. Protección de la información y de los bienes informáticos

4.1.1. El usuario, funcionario o contratista deberá reportar de forma inmediata a la Dirección de TIC cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

4.1.2. El usuario, funcionario o contratista tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

### 4.2. Controles de acceso físico

4.2.1. Cualquier persona que tenga acceso a las instalaciones del Fondo de Vigilancia y Seguridad, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, las cuales podrá retirar el mismo día. En caso de exceder las 24 horas, deberá tramitar la autorización de salida correspondiente en el área en la cual labora o a la cual visitó.

4.2.2. Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, propiedad del Fondo de Vigilancia y Seguridad, podrá ser retirado de las instalaciones únicamente con la autorización de salida del área correspondiente, anexando el comunicado de autorización del equipo debidamente firmado por un cargo no inferior a Director.

### 4.3. Seguridad en Data Center

4.3.1. Los Centros de Cómputo del Fondo de Vigilancia y Seguridad son áreas restringidas, por lo que solo el personal autorizado por la Dirección de TIC puede acceder a él.

### 4.4. Protección y ubicación de los equipos

4.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Dirección de TIC, en caso de requerir este servicio deberá solicitarlo a la mesa de ayuda.

4.4.2. El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Dirección de TIC.

4.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores del Fondo de Vigilancia y Seguridad.

4.4.4. Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro destinada ello y la cual es diferente para archivos de programas y sistemas operativos.

4.4.5. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

4.4.6. Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

4.4.7. Se debe mantener el equipo informático en un lugar limpio y sin humedad. El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.




Carrera 7 No. 32 – 12 Edificio
Centro Comercial San Martín
Pisos 33 a 36 Bogotá D.C.
Colombia
Código postal: 111711

## 5. ADMINISTRACIÓN DE OPERACIONES EN EL DATA CENTER Y LOS CENTROS DE CABLEADO

### 5.1. Responsabilidad

La Dirección de TIC en cabeza del Director, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.

### 5.2. Controles

5.2.1. Cuando un funcionario no autorizado o un visitante tengan la necesidad de ingresar al Data Center, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno del Administrador del Centro de Datos, y donde se especifique tipo de actividad a realizar. Se debe contar con la presencia de un funcionario de la Dirección de TIC de manera permanente en caso que se trate de un visitante externo.

5.2.2. El administrador del Centro de Datos deberá llevar un registro escrito de todas las visitas autorizadas a los Centros de Cómputo restringidos.

5.2.3. Todo equipo informático ingresado a los Centros de Cómputo restringidos deberá ser registrado en el libro de visitas.

5.2.4. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

5.2.5. La Dirección de TIC estará encargada de proveer los elementos de protección necesarios para el Data Center, tales como control de acceso, CCTV, sistema extintor de incendios, Sistemas ininterrumpidos de potencia y demás que sean necesarios para la normal operación del centro de cómputo.

## 6. SEGURIDAD LOGICA

### 6.1. Uso de medios de almacenamiento

6.1.1. Es responsabilidad del usuario, funcionario o contratista evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

6.1.2. Los usuarios y servidores del Fondo de Vigilancia y Seguridad deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

6.1.3. El uso de medios de almacenamiento extraíbles (discos duros, pendrives, unidades cd CD-DVD-Blu-ray) se encuentra restringido. En caso de requerirse una excepción, deberá solicitarse por escrito a la Dirección de TIC indicando claramente las razones laborales que justifican el requerimiento, la cual deberá estar firmada por el jefe inmediato con cargo no inferior a Director.

### 6.2. Uso de software Comercial y control de licenciamiento

6.2.1. Se prohíbe de instalación de software y programas no autorizados y sin licencia. Para el Control de Licenciamiento de Software, la Dirección TIC podrá hacer uso de agentes de software que reporten en línea y tiempo real los programas o aplicaciones instaladas en los equipos de cómputo del Fondo de Vigilancia y Seguridad.

6.2.2. Los usuarios y funcionarios que requieran la instalación de software del cual se tenga licencia o sea propiedad del Fondo de Vigilancia y Seguridad, deberán justificar su uso y solicitar su autorización a la Dirección de TIC con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

6.2.3. Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red

del Fondo de Vigilancia y Seguridad sin que esté autorizado por la Dirección de TIC.

6.2.4. Todos los certificados de licenciamiento, y paquetes de medios de instalación serán custodiados y almacenados por la Dirección de TIC.

### 6.3. Uso y seguridad de la Red

6.3.1. Los usuarios de la red del Fondo de Vigilancia y Seguridad no deberán establecer redes de área local propias, conexiones remotas a redes internas o externas, ni intercambio de información con otros equipos de cómputo utilizando protocolos de transferencia de archivos, sin la autorización de la Dirección de TIC.

6.3.2. No está permitido el uso de conexiones personales a Internet (módems, MiFi o conexiones compartidas desde smartphones) desde los equipos que se encuentran conectados a la red LAN o WiFi del Fondo de Vigilancia y Seguridad.

6.3.3. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección de TIC, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del Fondo de Vigilancia y Seguridad, así como las aplicaciones que sobre dicha red operan con fines de detectar y explotar una posible vulnerabilidad en sistemas operativos, sniffers o herramientas de man in the middle.

6.3.4. La administración remota de equipos conectados a Internet a través de la red LAN no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y por la Dirección de TIC.

### 6.4. Política de Uso del Correo electrónico

6.4.1. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la Entidad. Es decir, para transmitir información que tenga que ver única y exclusivamente con el buen

desarrollo de nuestras funciones.

6.4.2. Los contenidos del sistema de correo electrónico pertenecen a la Entidad y los mensajes electrónicos podrán ser leídos sin previo aviso por las dependencias de control.

6.4.3. La descarga de software o apertura de archivos ejecutables provenientes desde un correo externo se encuentra totalmente prohibida.

6.4.4. Se prohíbe el envío mediante correo electrónico de toda publicidad o cualquier tipo de aviso comercial no solicitado previamente por el destinatario.

6.4.5. No se podrá usar el formato HTML e imágenes que puedan generar daños en la cuenta de correo electrónico del destinatario.

6.4.6. Se deberán usar programas de compresión de datos (zip) para archivos adjuntos en dichos avisos.

6.4.7. Queda expresamente prohibido a cualquier cliente o usuario la utilización del servidor de correo de otro sitio para retransmitir correo sin el permiso expreso del sitio das.gov.co (Relaying).

6.4.8. A todos los clientes o usuarios se les notifica que está terminantemente prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam o correo no deseado.

6.4.9. Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del Orden Público, la moral, las buenas costumbres nacionales e internacionales, los usos y costumbres aplicables en Internet y el respeto de los derechos de terceras personas.

### 6.5. Políticas de Uso de Internet

6.5.1. El acceso a Internet provisto a los usuarios y funcionarios del Fondo de Vigilancia y Seguridad es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

6.5.2. Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Fondo de Vigilancia y Seguridad.

6.5.3. Los usuarios de Internet del Fondo de Vigilancia y Seguridad tienen que reportar todos los incidentes de seguridad informática a la Dirección de TIC inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

6.5.4. La Dirección de TIC podrá implementar herramientas automáticas de control de contenido que restringirán el acceso a páginas no autorizadas y realizarán el monitoreo de todas las conexiones que se realicen desde la red del Fondo de Vigilancia y Seguridad hacia redes externas e Internet.

6.5.5. Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

***Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.***

***Saben que existe la prohibición de descarga de software sin la autorización de la* Dirección de TIC*.***

***La utilización de Internet es para el desempeño de sus funciones y cargo en el Fondo de Vigilancia y Seguridad y no para propósitos personales.***

## 7. ADMINISTRACIÓN DE USUARIOS Y ROLES

**POLÍTICA:** Cada usuario, funcionario o contratista es responsable de los mecanismos de control de acceso que les sean proporcionados; esto es, de su “ID” login de usuario y contraseña necesarios para acceder a la red interna de información, a la infraestructura tecnológica o a las aplicaciones del Fondo de Vigilancia y Seguridad.

### 7.1. Administración y uso de contraseñas

7.1.1. Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

7.1.2. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección de TIC antes de poder usar la infraestructura tecnológica de la Fondo de Vigilancia y Seguridad.

7.1.3. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Fondo de Vigilancia y Seguridad.

7.1.4. Cada usuario que acceda a la infraestructura tecnológica del Fondo de Vigilancia y Seguridad debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

7.1.5. Los usuarios, funcionarios y contratistas son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

7.1.6. Las contraseñas de acceso a la red, así como de ingreso a las aplicaciones estarán regidos por la siguiente política: Mínimo 8 caracteres que incluyan al menos una letra mayúscula, una letra minúscula, un número y un carácter especial. El sistema automáticamente exigirá cambiar la contraseña cada 90 días calendario y no permitirá asignar las tres últimas contraseñas usadas. En caso de ingresar una contraseña herrada en tres ocasiones consecutivas, el sistema bloqueará indefinidamente el usuario.

7.1.7. La dirección de TIC será la encargada de administrar las políticas de seguridad de la red de dominio, donde se deberá incluir la política de contraseñas, el bloqueo automático de sesión por ausencia después de 10 minutos de inactividad, la restricción a medios extraíbles y las restricciones a las configuraciones locales de los sistemas operativos.




Carrera 7 No. 32 – 12 Edificio Centro Comercial San Martín Pisos 33 a 36 Bogotá D.C. Colombia
Código postal: 111711

7.1.8. La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

7.1.9. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir a la Dirección de TIC y solicitar el desbloqueo o cambio de contraseña a través de la mesa de ayuda. No se permitirán solicitudes efectuadas por terceros.

7.1.10. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

7.1.11. Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

7.1.12. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

7.1.13. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

### 7.2. Administración de Roles y Privilegios

7.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la Dirección de TIC (Administrador de la Red), para el cambio de privilegios mediante comunicación escrita firmada por el jefe inmediato con cargo no inferior a Director.

### 7.3. Controles para Otorgar, Modificar y Retirar Accesos a Usuarios

7.3.1. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro de los sistemas de Información del Fondo de Vigilancia y Seguridad, deberá ser solicitada de manera formal por escrito en versión física o por correo electrónico dirigido a soporte.tecnico@fvs.gov.co, solo se aceptarán solicitudes provenientes del jefe inmediato con cargo no inferior al de Director.

7.3.2. La Dirección de TIC, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios con base a las solicitudes.

## 8. CONTROLES CONTRA VIRUS O SOFTWARE MALICIOSO

**POLITICA:** La Dirección de TIC será la encargada de proveer, instalar, configurar y mantener actualizado el software de protección antivirus y de malware en los equipos propiedad del Fondo de Vigilancia y Seguridad.

8.1.1. Para prevenir infecciones por virus informático, los usuarios del Fondo de Vigilancia y Seguridad no deben hacer uso de software que no haya sido proporcionado y validado por la Dirección de TIC.

8.1.2. Los usuarios del Fondo de Vigilancia y Seguridad deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Dirección de TIC.

8.1.3. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar a la Dirección de TIC para la revisión y erradicación del virus.

8.1.4. Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Dirección de TIC en: Antivirus, Outlook, office, Navegadores u otros programas.

8.1.5. Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario del Fondo de Vigilancia y Seguridad, distinto al personal de la Dirección de TIC deberá intentar erradicarlos de las computadoras.

## 9. CLÁUSULAS DE CUMPLIMIENTO

9.1.1. La Dirección de TIC realizará acciones de verificación del cumplimiento de las Políticas y Estándares de Seguridad Informática.

9.1.2. La Dirección de TIC podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.

## 10. VIOLACIONES DE SEGURIDAD INFORMÁTICA

10.1.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática.

10.1.2. Ningún usuario o funcionario del Fondo de Vigilancia y Seguridad debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección de TIC.

10.1.3. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Fondo de Vigilancia y Seguridad.

## 11. IDENTIFICACIÓN DE INCIDENTES DE SEGURIDAD INFORMATICA

11.1.1. El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo a la Dirección de TIC lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

11.1.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar de manera inmediata a la Dirección de TIC.