MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

PROCESO DE REVISION: 28/AGOSTO/2018

Contenido

INTRODUCCIÓN

Los avances en Internet, los desarrollos informáticos y las telecomunicaciones han llevado a que muchas organizaciones gubernamentales y no gubernamentales desarrollen políticas que norman el uso adecuado de estas tecnologías y recomendaciones para evitar el uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

Por ello la Seguridad Informática se ha convertido, en un tema de especial relevancia para cualquier persona que tenga contacto con las Tecnologías de Información y Comunicaciones. Una administración eficiente de los recursos informáticos para la protección, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones.

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de informático con el fin de proteger y resguardar su funcionamiento y la información contenida en él. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban principalmente enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente el Instituto Superior de Auditoria y Fiscalización cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo, aplicaciones, y servidores que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Al ser la información institucional un activo muy valioso para la Entidad, se hace necesaria no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Este compendio tiene como finalidad dar a conocer las PSI - Políticas de Seguridad Informática, que deben aplicar y acatar los empleados del Instituto Superior de Auditoria y Fiscalización, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos.

OBJETIVOS DE LA POLÍTICA

Establecer las Políticas y Estándares de Seguridad de las Tecnologías de la Información en el ISAF, las cuales son el fundamento para proteger la integridad, el control efectivo y resguardo de la información, así como las actividades de los funcionarios y empleados del Instituto que son realizadas a través de operaciones de cómputo o del uso de equipos y recursos informáticos, proporcionando los procedimientos necesarios que permitan crear una "Cultura de Seguridad y Control de la Información" y nos ayude a tomar conciencia de la importancia de proteger la Información, el Hardware, el Software, las redes de datos y comunicaciones del ISAF.

ALCANCE

Los Empleados

La seguridad informática es un esfuerzo grupal. Esto requiere de la participación y el esfuerzo de todos los miembros del ISAF que trabajan con sistemas de información. Por lo que cada empleado deberá comprometerse en el cumplimiento de los requisitos de la Política de Seguridad Informática.

Los Sistemas (Hardware y Software)

Esta Política aplica para todos los equipos de cómputo, redes, aplicaciones y sistemas operativos que son propiedad o son operados por el ISAF. La Política cubre únicamente la información manejada por los equipos de cómputo y las redes institucionales.

Contratistas

Se definen como contratistas a aquellas personas que han suscrito un contrato con la Entidad y que pueden ser:

- Colaboradores por Outsourcing: son aquellas personas que laboran en la ISAF y tienen contrato con empresas de suministro de servicios y que dependen de ellos.
- Personas naturales que prestan servicios independientes al ISAF.
- Proveedores de recursos informáticos.

DEFINICIONES

Para efectos del presente documento se entiende por:

ISAF: Hace al Instituto Superior de Auditoría y Fiscalización.

DGTI: Hace referencia a la Dirección General de Tecnologías de la Información.

Política de Seguridad Informática: Consiste en asegurar que los recursos y la información soportada en la plataforma informática (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. Toda intención y directriz expresada formalmente por la alta dirección.

Confidencialidad: Es asegurar que la información sea utilizada sólo por las personas autorizadas para ello.

Integridad: Mantenimiento de la exactitud e integralidad de la información y sus métodos de proceso.

Software Malicioso: Programa o parte de un programa destinado a perturbar, alterar o destruir la totalidad o parte de los elementos de la lógica esencial para el funcionamiento de un sistema de procesamiento de la información. Estos programas se pueden dividir en cuatro clases: los virus informáticos, gusanos, troyanos y bombas lógicas.

Amenaza: Es un evento que puede desencadenar un incidente en el sistema informático, produciendo daños materiales o pérdidas inmateriales en sus activos.

Riesgo: Es la probabilidad de ocurrencia de un hecho favorable o desfavorable que pudiera afectar la Seguridad Informática.

Vulnerabilidad: Son aspectos que influyen negativamente en la Seguridad Informática y que posibilitan la materialización de una amenaza.

Ataque: Evento, exitoso o no que atenta sobre el buen funcionamiento del Sistema Informático.

Sistema de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

Incidente de Seguridad Informática: Es un evento atribuible a una causa de origen humano. Esta distinción es particularmente importante cuando el evento es el producto

de una intención dolosa de hacer daño. Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un Sistema Informático.

Buzón: También conocido como Cuenta de correo electrónico o de E-Mails.

Dispositivos USB: Es un dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas).

Contraseña o Clave: Es una forma de autenticación o control de acceso que utiliza información secreta para controlar el acceso hacia algún recurso informático. Puede está conformado por números, letras y/o caracteres especiales

Virus: Es un programa de ordenador que puede copiarse a sí mismo e infectar un ordenador.

Sistema Multiusuario: Se refiere a un concepto de sistemas operativos, pero en ocasiones también puede aplicarse a programas de ordenador de otro tipo (e.j. aplicaciones de base de datos). En general se le llama Multiusuario a la característica de un Sistema Operativo o Programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente.

FTP: (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos): En informática es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

Información confidencial (CONFIDENCIAL): Información generada por el ISAF en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por el ISAF cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información pública: Es la información administrada por el ISAF en cumplimiento de sus deberes y funciones que está a disposición del público en general.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

SENSIBILIDAD Y CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información constituye un elemento importante para la administración del riesgo, ya que determina la prioridad y el grado de protección requerido para cada tipo de información que repose en los sistemas informáticos.

La DGTI ha definido unos criterios para la clasificación de la información que reposa en la plataforma informática. Estos criterios establecen el nivel apropiado de protección para cada una de las categorías e informa a los empleados responsables de cualquier medida especial o tratamiento requerido. Toda la información del Sistema Informático debe estar clasificada dentro de los siguientes criterios:

1. Confidencial: Hace referencia a aquella información que solamente puede ser conocida y manejada por personal expresamente autorizado.

2. De Uso Interno: Información que puede ser de libre utilización por los empleados del Instituto para llevar a cabo las actividades laborales.

3. Pública: Es aquella información que podrá ser utilizada o conocida por todos los empleados del ISAF e, incluso, por terceros.

Para garantizar la Seguridad Informática todos los empleados deben familiarizarse con la definición de cada categoría, así como también con las medidas aplicadas.

POLÍTICAS GENERALES DE SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN

1. POLÍTICAS DE SEGURIDAD PERSONAL

1.1 Obligaciones de los Empleados

Es responsabilidad de los usuarios de equipos de cómputo y servicios de T.I. del ISAF, cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

Los empleados deben tomar conciencia de la importancia del establecimiento de la Política de Seguridad Informática, los procedimientos y la normatividad aplicable. Estas normas deben ser completamente entendidas y aplicadas en la cotidianidad de sus tareas.

Los empleados que sean responsables de la información deben establecer medidas de seguridad con base en la información que se encuentre a su cargo.

Los empleados que sean responsables de la información deben establecer la clasificación que mejor refleje el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información que se encuentre bajo su cuidado. Esta clasificación determinará el nivel de acceso a los empleados.

Los empleados, además de ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus tareas.

Son responsables por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que otra persona realice labores bajo su identidad. De forma similar, los empleados y usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad del ISAF.

Los empleados responsables de información que utilicen equipos portátiles deberán almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente hacer copias de respaldo y así evitar la pérdida de información crítica en caso de algún robo o extravió, en caso de requerir asesoría puede solicitarla a la DGTI.

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de equipos de cómputo y servicios de T.I. del ISAF deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información del ISAF, así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.3 Declaración de reserva de derechos del ISAF.

El Instituto usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por sus computadoras y sistemas de información. Para mantener estos objetivos del ISAF se reserva el derecho y la autoridad de:

1. Restringir o revocar los privilegios de cualquier usuario;
2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados;
3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información del ISAF.

Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad de la DGTI y se cuente con el consentimiento del Auditor Mayor del ISAF.

2. POLÍTICAS DE ACCESO A INFORMACIÓN Y DIVULGACIÓN DE SEGURIDAD

2.1 Acceso de información por parte de Terceros

El acceso a terceros de la información del Instituto quedará estrictamente prohibido y solo será permitido siempre y cuando haya la debida autorización del Auditor Mayor del ISAF.

Cuando el suministro de la información involucre aspectos tecnológicos deberá contarse adicionalmente con el visto bueno previo de la DGTI, quien deberá validar los riesgos de la seguridad de la información requerida.

2.2 Divulgación de la seguridad de la información a personal externo

La información relativa a las medidas de seguridad, a los sistemas de procesamiento de información y a las redes es confidencial y no debe ser divulgada a usuarios no autorizados a menos que se cuente con la autorización de la DGTI.

3. POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

3.1 Control de Acceso a la Información

3.1.1. El acceso al centro de datos, servidores y áreas de trabajo que contengan información sensible o crítica, como la contenida en los servidores, debe estar restringido y solamente el personal autorizado por la DGTI podrá acceder a estos lugares.

3.1.2. La información sensible o crítica debe estar siempre protegida contra la divulgación no autorizada.

3.1.3. Documentos impresos que contengan información sensible o crítica deben estar siempre almacenados o guardados en lugares que garanticen su seguridad, conservación y protejan su acceso inclusive durante horas no laborales.

3.1.4. Siempre que no se esté utilizando su equipo de cómputo debe cerrarse la sesión de trabajo para evitar que un empleado no autorizado acceda al sistema.

3.1.5. El empleado tiene la obligación de proteger los discos, CD-ROM y otros medios de almacenamiento como memorias USB que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

3.1.6. Es responsabilidad del empleado evitar en todo momento la fuga de la información del ISAF que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

3.1.7. Las computadoras de escritorio, proyectores y/o cualquier activo de tecnología de información del ISAF sólo podrá ser retirado de las instalaciones con la autorización de la Dirección General de Administración o la DGTI.

3.1.8. Los empleados no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de estos sin la autorización respectiva de la Dirección General de Administración.

3.1.9. La Dirección General de Administración será la encargada de generar el resguardo y recabar la firma del empleado como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la DGTI. El movimiento o retiro de equipos por traslado, reemplazo o baja debe ser informado a la Dirección General de Administración, por la DGTI y el empleado responsable del activo.

3.1.10. El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones del ISAF.

3.1.11. Será responsabilidad del empleado solicitar a la DGTI la asesoría necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

3.1.12. Mientras se opera el equipo de cómputo no se deberán consumir alimentos y/o ingerir líquidos sin tomar las debidas precauciones para evitar posibles daños en estos, de ocurrir algún daño derivado de esto, la Dirección General de Administración será la que determine la sanción.

3.1.13. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.

3.1.14. Se debe mantener el equipo de cómputo en un entorno limpio y sin humedad.

3.1.15. El empleado debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

3.1.16. Queda prohibido que el usuario abra o desarme los equipos de cómputo. Únicamente el personal autorizado por la DGTI podrá llevar a cabo los servicios y reparaciones al equipo de cómputo.

3.1.17. Los empleados y la DGTI, deberán asegurarse de respaldar la información que consideren relevante y borrarla cuando el equipo de cómputo sea enviado a garantías y/o reparaciones, evitando así la pérdida involuntaria de información, derivada del proceso de reparación.

3.1.18. El empleado que tenga bajo su custodia algún equipo de cómputo será responsable de su uso y conservación; en consecuencia, responderá con su propio patrimonio por la pérdida, daño o deterioro que ocurra a los equipos cuando el hecho acontezca por negligencia o culpa del trabajador.

3.1.19. El resguardo para los portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

3.1.20. El empleado deberá dar aviso inmediato de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo a la Dirección General de Administración.

3.1.21. El empleado que tenga bajo su resguardo dispositivos especiales es responsable del buen uso que se les dé.

3.1.22. Si algún área por requerimiento muy específico tiene la necesidad de contar con un dispositivo especial o específico, su instalación deberá ser autorizada por el Auditor Mayor, con el apoyo técnico de la DGTI.

3.1.23. Deberá configurarse el equipo de cómputo de tal manera que durante un tiempo de inactividad éste sea bloqueado automáticamente y se requiera para el reinicio de actividades el ingreso de una clave o contraseña, el tiempo de inactividad se ha establecido en 5 minutos.

3.1.24. Datos sensibles enviados a través de redes externas deben estar encriptados. Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados. La DGTI brindará asesoría para realizar el proceso de Cifrado.

3.1.25. Eliminación Segura de la Información en medios Informáticos: Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por el ISAF, antes de su entrega se les realizara un proceso de borrado seguro en la información.

3.1.26. Eliminación segura de la información en medios físicos: Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva máquina destruye papel o cualquier otro método seguro de destrucción.

3.2 Protección contra robo

3.2.1. Los sistemas, equipos de red y dispositivos USB deben asegurarse físicamente cuando se encuentren en oficinas o lugares abiertos.

3.2.2. Tanto los equipos de red, servidores y otros sistemas multiusuario deben estar ubicados en lugares con control de acceso.

3.2.3. Los equipos portátiles deben ubicarse en gabinetes cerrados o asegurados cuando se encuentren en lugares no vigilados.

3.2.4 En lo posible, utilice un software de cifrado para resguardar con mayor seguridad los datos almacenados en su portátil, para ello, es recomendable elegir una frase larga, contraseña de cifrado fuerte y mantenerlos seguros. La DGTI le brindará la información y asesoría necesaria para llevar a cabo esta actividad. De esta manera, si su portátil se pierde o es robado, la configuración de cifrado proporciona una protección muy fuerte contra el acceso no autorizado a los datos.

3.2.5. El empleado que sospeche o tenga conocimiento de un incidente de seguridad informática deberá reportarlo al Jefe Inmediato y a la DGTI lo antes posible, indicando claramente los datos por los cuales lo considera un riesgo.

3.2.6. Cuando exista la sospecha o el conocimiento que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización debida, el empleado deberá notificar a su Jefe Inmediato y a la DGTI.

3.2.7. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del ISAF debe ser reportado a la Dirección General de Administración y a la DGTI.

4. POLÍTICAS DE CONTROLES DE ACCESO LÓGICO Y FISICO.

4.1 Usuario y Clave

4.1.1. El ISAF a través de la DGTI requiere que todos los empleados que tengan acceso a sus recursos tecnológicos como Sistemas y Servicios en la red interna dispongan de un Usuario y una Clave de carácter privado, personal e intransferible.

4.1.2. La asignación del Usuario y Clave debe estar acorde a las funciones, responsabilidades y actividades del usuario.

4.1.3. Todos los empleados tienen la obligación de proteger sus datos de autenticación.

4.1.4. El acceso a la infraestructura tecnológica del ISAF para personal externo debe ser autorizado por el Auditor Mayor, el cual notificará a la DGTI para la habilitación.

4.1.5. Está prohibido que los empleados utilicen la infraestructura tecnológica del ISAF para obtener acceso no autorizado a la información o a otros sistemas de información del ISAF.

4.1.6. Todos los empleados deberán utilizar el Usuario y Clave provistos por la DGTI antes de poder usar la infraestructura tecnológica del ISAF.

4.1.7. Los empleados no deben proporcionar información a personal externo de los mecanismos de control de acceso a la infraestructura tecnológica del ISAF, a menos que se tenga la autorización del Auditor Mayor.

4.1.8. Cada empleado que acceda a la infraestructura tecnológica del ISAF debe contar con un Usuario único y personalizado, por lo cual no está permitido el uso de un mismo Usuario por varios empleados.

4.1.9. Cualquier cambio en los roles y responsabilidades de los empleados que modifique sus privilegios de acceso a la infraestructura tecnológica del ISAF deberá ser notificado a la DGTI con el visto bueno de su Jefe Inmediato.

4.1.10. La asignación de la Clave para los sistemas y acceso de red debe ser realizada en forma individual, por lo que el uso de claves compartidas está prohibido.

4.1.11. Cuando un empleado olvide, bloquee o extravíe su Clave deberá informarlo a la DGTI para que se le proporcione una nueva Clave y una vez que la reciba deberá cambiarla en el momento en que acceda nuevamente a la infraestructura tecnológica.

4.1.12. Está prohibido que las Claves se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

4.1.13. Sin importar las circunstancias, las Claves nunca se deben compartir o revelar. Hacer esto responsabiliza al empleado que prestó su Clave de todas las acciones que se realicen con la misma.

4.1.14. Las Claves iniciales para los sistemas informáticos tendrán una vigencia de 15 días. Finalizando este periodo la DGTI cambiará la contraseña para obligar al usuario a proporcionar su propia contraseña segura. Si el empleado llegara a sospechar que su Clave ha sido descubierta deberá modificarla inmediatamente.

4.1.15. Los empleados no deben almacenar las claves en ningún programa o sistema que proporcione esta facilidad.

4.1.16. Las claves no deben ser guardadas en archivos que puedan ser leídos, computadores sin control de acceso o en lugares donde personal no autorizado tenga acceso.

4.2 Elección de una Clave

Los empleados deben elegir una Clave que sea difícil de adivinar y que no contenga información relativa a la vida personal. Por ejemplo, no debe contener el número de la cédula, la fecha de nacimiento, número de teléfono, nombre de familiares (esposa, esposo, hijo), nombre de la mascota, etc.

4.2.1. Algunos consejos para la creación de claves o contraseñas.

4.2.1.1. Deben estar compuestos de al menos seis (6) caracteres. Estos caracteres deben ser contener alfanuméricos.

4.2.1.2. Combinar varias palabras. Combinar palabras con signos de puntuación o números, caracteres mayúsculas y minúsculas.

4.2.1.3. Transformar una palabra común utilizando un método específico y personal.

4.2.1.4. Crear acrónimos.

4.2.1.5. Deliberadamente utilizar mal una palabra o escribirla mal ortográficamente.

4.2.1.6. No deben ser idénticos o similares a claves o contraseñas que hayan sido usados previamente.

4.2.1.7. No utilice la misma clave para los diferentes sistemas o puntos de acceso al que esté autorizado.

4.2.1.8. Las claves en ningún momento deben ser compartidas o divulgadas.

4.2.1.10. Si se advierte que un empleado está utilizando los datos de autenticación (Usuario y Clave) de otro empleado, es su responsabilidad avisar de este evento a su Jefe Inmediato y a la DGTI.

5. POLÍTICAS DE ADMINISTRACIÓN DE TECNOLOGIAS DE LA INFORMACION.

5.1 Uso de los recursos tecnológicos de la institución

Todos los empleados que utilicen los sistemas de procesamiento de información o los recursos del ISAF deberán actuar basados en las normas establecidas en la Política de Seguridad informática.

Los sistemas de información del ISAF deberán ser utilizados exclusivamente con fines institucionales.

El uso con fines personales de los recursos tecnológicos del ISAF estará permitido siempre y cuando sea autorizado por su Director de Área, en tiempo no laboral y no afecte la productividad ni la seguridad de la información de la institución.

Se prohíbe la utilización de las computadoras y recursos del ISAF para ejecutar juegos de cualquier índole. Estas actividades darán lugar a acciones disciplinarias.

5.2 Derechos de Investigación Forense

La DGTI, previa autorización del Auditor Mayor del Instituto, se reservará el derecho de investigar e inspeccionar en cualquier momento los sistemas de información utilizados por los empleados, con el fin de detectar actos que incumplan con los valores del ISAF.

Las inspecciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado.

Los Sistemas de Información sujetos a dicha inspección incluyen los registros de la actividad de los empleados: archivos y correos electrónicos institucionales y soportes físicos de la información auditada pueden ser sujetos de la misma inspección en cualquier momento.

Lo anterior, sin perjuicio del respeto a la intimidad personal y a la inviolabilidad de la correspondencia y demás formas de comunicación privada en los términos del mandato constitucional.

El ISAF se reserva el derecho de retirar cualquier material lesivo para los intereses de la institución o que contenga información ilegal.

5.3 Declaración de Propiedad Exclusiva

EL ISAF tiene propiedad y derechos exclusivos sobre las patentes, derechos de autor, invenciones, programas o cualquier otra propiedad intelectual desarrollada por sus empleados en la plataforma tecnológica de la entidad.

5.4 Acceso a Internet

Todos los empleados del ISAF con sistemas de información asignados tendrán acceso a Internet desde sus estaciones de trabajo. El instituto se reserva el derecho de retirar o restringir dicho acceso.

El acceso a Internet podría llegar a ser monitoreado por la DGTI para asegurar el uso apropiado y el cumplimiento de las Políticas de Seguridad, si se detecta algún incumplimiento a la Política de Seguridad.

El Instituto dispone de un software para el control de la navegación en Internet, el cual restringe el acceso a las categorías que universalmente las instituciones bloquean como por ejemplo sitios de contenido pornográfico, consumo de ancho de banda, contenidos racistas, violencia, ocio, etc. Dicho software podrá generar Reportes de los resultados (loggs) de la navegación, los cuales podrían ser enviados a los Directores de Área, Auditor Mayor o Contraloría Interna, si así lo requieran para realizar un respectivo análisis y seguimiento de Uso de Internet.

De necesitarse el bloqueo de alguna página de internet deberá ser autorizada por el Auditor Mayor del Instituto, para que con ello la DGTI proceda a realizar dicha solicitud.

El acceso a Internet provisto a los usuarios del ISAF es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

Todos los accesos a Internet tienen que ser realizados a través de los accesos provistos por la DGTI. En caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada y aprobada por la DGTI.

Los empleados del ISAF con acceso a Internet tienen que reportar todos los incidentes de seguridad informática a la DGTI inmediatamente después de su identificación.

Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga de archivos multimedia (audio y/o videos), P2P, Torrent entre otros, si se detecta el uso de alguno de ellos se podrán ejecutar sanciones y restricciones de uso de internet.

Los empleados del ISAF con acceso a Internet, al acceder al servicio están aceptando que:

1. Podrían ser sujetos de monitoreo de las actividades que realizan en Internet.

2. Existe la prohibición de acceso a páginas no autorizadas.

3. Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.

4. Se prohíbe la descarga de software sin la autorización de la DGTI.

5. La utilización de Internet es para el desempeño de su función en el Instituto y no para propósitos personales.

5.5 Correo Electrónico

El ISAF ofrece un servicio de correo electrónico institucional para facilitar la comunicación y ejecución de sus actividades.

El intercambio de correos relacionados con las actividades del ISAF deberá ser a través de los buzones institucionales. Está prohibido tramitar información institucional a través de e-mails privados o de uso personal (Gmail, Hotmail, etc.).

El tamaño para los contenidos de los archivos adjuntos enviados por email no podrá exceder 25 MB (megas); de presentarse casos que exceden esta capacidad deberá acudir o comunicarse a la DGTI para auxiliarlo en otro tipo de método para compartir sus archivos mediante el mismo correo electrónico. Es decir, por defecto, no podrá enviarse

un email o correo electrónico cuya sumatoria de los tamaños de los archivos adjuntos del mismo exceda los 25 MB (Megas).

La firma establecida para los emails deberá informar: El nombre de la institución, el cargo del empleado que envía el email, el teléfono y extensión.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

Software e información sensible del ISAF que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

Los empleados no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.

Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el director de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia, así mismo comunicar en qué momento detener el reenvió de correos.

Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos que reciba a través del correo institucional como información de propiedad del ISAF.

Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Está prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

5.6 Manejo de Licencias

Únicamente se autoriza la instalación de software que se encuentre soportado con su respectiva licencia. La adquisición de software nuevo deberá ser autorizada por el Auditor Mayor, para después ser supervisada por la DGTI.

No se permite descargar, instalar o utilizar programas de software no autorizadas. Esta práctica, podría introducir serias vulnerabilidades de seguridad en las redes, sistemas e información del ISAF, además de afectar el funcionamiento de su computador.

Los paquetes de software que permiten que el equipo sea manejado a control remoto (por ejemplo, TeamViewer, PCAnywhere) y herramientas para hacking (por ejemplo, sniffers, crackers) están explícitamente prohibidos, a menos que hayan sido expresamente autorizados previamente por el Auditor Mayor y a su vez aprobados por la DGTI.

Respecto a las licencias de software. La mayoría del software, a menos que esté específicamente identificado como "freeware" o "software de dominio público", sólo puede ser instalado y / o utilizarse si ha sido validado por la DGTI. Paquetes de shareware o de prueba deben ser aprobados por la DGTI y eliminados una vez haya expirado el período de prueba. Algunos programas de software son sólo para uso libre de los particulares, mientras que el uso comercial o empresarial requiere un pago de licencia.

El ISAF no permite materiales inapropiados, como los archivos pornográficos, racistas, difamatorios o de acoso, fotos, videos o mensajes de correo electrónico que pueda causar ofensa o vergüenza. No está permitido almacenar, usar, copiar o distribuir este material en los computadores de la organización.

El DGTI podrá en cualquier momento validar que el software instalado en una computadora se encuentre legalmente soportado con su respectiva licencia. De dicha inspección se pasará un reporte al Auditor Mayor y/o director área con el fin de informar la relación, el estado y legalidad del software instalado.

LA DGTI determinará la conveniencia o no de la instalación de un determinado software en un computador.

Los empleados que requieran la instalación de software que no sea propiedad del ISAF deberán justificar su uso y solicitar su autorización a la DGTI, indicando el equipo de cómputo donde se instalará el software, el propósito y el período de tiempo que permanecerá dicha instalación, además de respaldar el mencionado software con la respectiva licencia de legalidad.

Las licencias deben ser custodiadas y controladas por la DGTI.

Se considera una falta grave que los empleados instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del ISAF, que no esté autorizado por el director del área respectiva y la DGTI.

5.7 Software de detección de virus

5.7.1. Los empleados no deberán cancelar los procesos automáticos de actualización de las definiciones de virus de Windows Defender.

5.7.2. Todos los archivos y/o software deben ser analizados por un antivirus se ha definido Windows Defender como el antivirus mínimo para el ISAF y/o de ser necesario utilizar otro externo.

5.7.3. Un análisis debe ser ejecutado antes de abrir un archivo nuevo y después de ejecutar un software nuevo. El antivirus instalado en el computador deberá garantizar este proceso de manera automática.

5.7.4. Para prevenir infecciones por virus informático los empleados del ISAF no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la DGTI.

5.7.5. Los empleados del ISAF deben verificar que la información y los medios de almacenamiento, considerando que al menos unidades USB y CD's estén libres de cualquier tipo de software malicioso o virus, para lo cual deben ejecutar el software antivirus autorizado por la DGTI.

5.7.6. Todos los archivos de computadora que sean proporcionados por personal externo o interno en relación con programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, deben ser verificados por el empleado de que estén libres de virus utilizando el antivirus autorizado antes de ejecutarse.

5.7.7. Ningún empleado del ISAF debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir códigos de computadora diseñados para auto replicarse, dañar, o, en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas del ISAF. El incumplimiento de este estándar será considerado una falta grave.

5.7.8. Ningún empleado o personal externo podrá bajar o descargar software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la DGTI.

5.7.9. Cualquier empleado que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la DGTI para la detección y erradicación del virus.

5.7.10. Cada empleado que tenga bajo su resguardo algún equipo portátil asignado por el ISAF y que dicho activo no esté conectado permanentemente a la red de internet

institucional, será responsable de solicitar periódicamente a la DGTI las actualizaciones de las definiciones de virus.

5.7.11. Los empleados no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el ISAF en: Antivirus, Outlook, Office, Navegadores u otros programas.

5.7.12. Todos los medios removibles y otros medios de almacenamiento electrónico sobre un equipo de cómputo infectado no deberán ser utilizados sobre otro equipo hasta que el virus haya sido removido de manera exitosa.

5.7.13. El equipo infectado deberá ser retirado de la operación para su revisión oportuna y efectiva.

5.7.14. Debido a que algunos virus son extremadamente complejos ningún empleado del ISAF debe intentar erradicarlos de las computadoras.

5.7.15. La DGTI será el encargado o responsable de llevar a cabo las acciones para la remoción del virus y garantizar la pérdida mínima de información, minimizar los daños y el tiempo fuera de servicio del computador infectado.

5.8 Seguridad de la RED

5.8.1. Conexiones a la red interna

5.8.1.1. Solo los equipos de cómputo del ISAF deberán estar conectados a la red institucional.

5.8.1.2. Los equipos conectados a la red interna deberán de contar con bloqueo automático por inactividad de 5 minutos y se deberá desactivar mediante contraseña definida por el usuario.

5.8.1.3. Los empleados no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del ISAF sin la autorización de la DGTI.

5.8.1.4. Será considerado como un ataque a la seguridad informática y una falta grave contra el ISAF cualquier actividad no autorizada por la DGTI en la cual los empleados

realicen la exploración de los recursos informáticos en la red del ISAF, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

5.8.2 Conexiones Remotas

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la DGTI y por su jefe directo.

5.8.3 Cambios en la red

5.8.3.1. Todos los cambios en la configuración de la red deben tener un registro que formalice dicho cambio y deben ser aprobados por la DGTI.

5.8.3.2. Todos los cambios a la red interna deben ser realizados por la DGTI. Este procedimiento reduce el riesgo de divulgación no autorizada y que los cambios realizados sean hechos de manera pertinente y con el conocimiento y aprobación del Director General de TI. Este proceso aplica no sólo al personal de ISAF, sino también a los proveedores de servicios o personal externo.

5.9 Trabajo Remoto, Teletrabajo o trabajo desde casa

Los empleados del ISAF podrán acceder de manera remota a los sistemas del ISAF procurando mantener la seguridad de la información, cuidando sus claves de acceso y a través de conexiones HTTPS en sus navegadores.

5.10 Servicios de Outsourcing – Subcontratación.

El Outsourcing, definido como la gestión o ejecución temporal o permanente de una función empresarial por un proveedor externo de servicios, debe ser controlado dado los riesgos potenciales que implica el acceso (Virtual o Físico) de éste a las instalaciones del ISAF, a la información, a los activos. Riesgos como por ejemplo el acceso inadecuado,

divulgación de información, impericia del subcontratista, pérdida de la propiedad intelectual, falta de apropiamiento (Sentido de Pertenencia), etc.

Se considera como proveedores de Outsourcing quienes:

1. Ofrecen soporte de Hardware y software y al personal de mantenimiento.
2. Consultores externos y contratistas.
3. Empresas TI de externalización de procesos empresariales.
4. Personal temporal

Cuando se requiera contratar servicios bajo el esquema de subcontratación, deben validarse los siguientes criterios o variables:

- Historia y reputación de la compañía.
- Calidad de los servicios provistos a otros consumidores.
- Número y competencias del personal y gerencia.
- Estabilidad financiera de la compañía y marca comercial.
- Rango de retención de empleados de la compañía.
- Garantía de calidad y normas de gestión de la seguridad que tiene actualmente la empresa.

Estas variables no son de obligatorio cumplimiento, pero si permiten generar confianza frente al proceso de subcontratación, con el fin de brindar mayores garantías respecto a la pertinencia del subcontratado.

En todos los casos, debe establecerse una relación contractual entre el ISAF y el tercero, dicha relación deberá ceñirse al Manual de Contratación documentado por el ISAF. En dicho contrato deberán indicarse, para los casos en que se haga necesario, instrucciones respecto a la protección de datos y normas de privacidad.

Si se intercambia información que es confidencial, se deberá generar o exigir un documento/acuerdo de confidencialidad entre la el ISAF y el Tercero, ya sea como parte del contrato de Outsourcing en sí o un acuerdo de confidencialidad por separado.

Se deben registrar o documentar los Controles de acceso para restringir la divulgación no autorizada, modificación o destrucción de la información, incluyendo controles de acceso físico y lógico, los procedimientos para conceder, revisar, actualizar y revocar el acceso a los sistemas, datos e instalaciones. Estos controles deben ser definidos entre la Dirección General de Administración y la DGTI con la aprobación del Auditor Mayor.

5.11 Dispositivos Móviles

Las nuevas tecnologías, en su constante evolución, han permitido que se desarrollen nuevas herramientas para desempeñar labores profesionales de forma más eficaz. Se ha evolucionado, del ordenador como principal herramienta de trabajo, a utilizar dispositivos móviles como smartphones o tablets en entornos de trabajo donde la movilidad es fundamental.

Sin embargo, esa movilidad conlleva unos riesgos asociados a la posibilidad de pérdida o robo del dispositivo, produciéndose una pérdida de confidencialidad de la información contenida en el mismo.

A continuación, se enumerarán algunas buenas prácticas o medidas disponibles que se pueden llevar a cabo para incrementar la seguridad en los dispositivos móviles.

5.11.1 Seguridad Lógica: Bloqueo por Contraseña.

La gran mayoría de dispositivos dispone de medidas de bloqueo al entrar en modo suspendido. Este recurso garantiza que el acceso al uso del dispositivo móvil sólo puede efectuarse por la persona autorizada que conoce la clave. En caso de extravío o robo, la única manera de poder utilizar el dispositivo es restaurando los valores de fábrica, por lo que toda la configuración y datos almacenados se perderían.

Existen varios métodos para restringir el uso del dispositivo. Éstos varían en función del fabricante. Los más utilizados son la contraseña con pin de 4 dígitos, contraseña alfanumérica o patrón de desbloqueo.

Es importante, igualmente, configurar el dispositivo móvil para que pasado un tiempo de inactividad pase automáticamente a modo de suspensión y se active el bloqueo de la pantalla. Si no se usara esta medida, la técnica de bloqueo perdería prácticamente toda su efectividad.

5.11.2 Cifrado de Memoria.

Esta práctica se suele complementar con la técnica anterior. Consiste en cifrar la memoria de almacenamiento, haciendo imposible la copia o extracción de datos si no se conoce la contraseña de desbloqueo.

Según el modelo o fabricante, se permite cifrar tanto la memoria interna como la memoria de almacenamiento externo, como las tarjetas de memoria flash.

Una vez cifrado, solo se podrá acceder a los datos almacenados al encender el dispositivo con la contraseña de bloqueo de pantalla. Si no se conociese la clave no sería posible recuperar la información, aunque se utilicen técnicas forenses de extracción y copia de datos.

La única forma posible sería con técnicas de fuerza bruta, que consisten en probar automáticamente todas las combinaciones posibles de contraseña, hasta encontrar aquella que permite el acceso. Por tanto, es importante que para que este ataque sea muy difícil de llevarse a cabo, se utilice una contraseña compleja, que combine letras con dígitos, mayúsculas y caracteres especiales.

5.11.3 Borrado Remoto.

Con esta práctica se podrán borrar los datos del dispositivo y restaurarlos a los valores de fábrica, todo ello de forma remota.

Puede ser muy importante tener a mano este recurso en caso de pérdida o robo del dispositivo, en el supuesto de que la información almacenada sea sensible. Esta función depende del tipo de dispositivo, del fabricante o de la operadora, y es posible que el servicio sea de pago.

5.11.4 Copias de Seguridad.

Si la información utilizada en el dispositivo es importante, y su pérdida ocasionara graves problemas, entonces sería conveniente utilizar alguna solución de copias de seguridad.

Hay programas que sincronizan los datos almacenados con el ordenador de escritorio, o en alguna aplicación online ofrecida por el fabricante, de forma que los datos están siempre disponibles y actualizados. En caso de pérdida del dispositivo, la información seguiría estando disponible y a salvo.

Se recomienda que, si se utilizan este tipo de opciones, de sincronizar los datos con alguna aplicación online externa a nuestra organización, no se sincronice la información confidencial si la hubiera, puesto que dejaría de “estar en nuestras manos”.

Lo recomendable es encontrar soluciones de copias de seguridad controladas por el ISAF, para que la información no viaje fuera de ella.

5.11.5 Los Peligros del Malware

El uso cada día más frecuente de smartphones y tablets ha derivado en que la creación de malware apunte hacia estas plataformas. Hoy día el riesgo de que un smartphone pueda ser infectado por un virus es una realidad. Éstos se basan principalmente en el robo de documentos, contraseñas, datos bancarios e información personal.

Por eso es conveniente adoptar unas políticas de seguridad para evitar en la medida de lo posible infecciones de malware que haga peligrar la confidencialidad, integridad y disponibilidad de la información. A continuación, se presentan algunas recomendaciones que apuntan a la mitigación de este riesgo:

5.11.5.1 Fuentes Confiables.

El principal problema de infecciones en dispositivos móviles es por causa de la instalación de programas desde fuentes desconocidas. Es muy importante instalar aplicaciones únicamente desde los repositorios oficiales del dispositivo, como App Store o Google Play y App World, para iPhone/iPad o Android y BlackBerry respectivamente.

Se debe evitar siempre instalar aplicaciones descargadas directamente de P2P, o foros. Se corre el serio riesgo de que estos programas contengan algún troyano y tras su instalación, infecten el dispositivo.

5.11.5.2 Jailbreak/root

Los términos Jailbreak o root de un dispositivo se refieren a conceder privilegios de administración a las aplicaciones, saltándose la protección que tiene por defecto los sistemas operativos. Esta característica puede añadir funcionalidades extra al dispositivo, pero también es un riesgo extra al que se expone, ya que se está eliminando la barrera de protección que sin jailbreak o root se mantiene.

Salvo que sea absolutamente necesario para el funcionamiento de una aplicación concreta, no se permite habilitar esta característica a los dispositivos.

5.11.5.3 Sólo las aplicaciones necesarias

Llenar el dispositivo de aplicaciones innecesarias no sólo ralentiza su funcionamiento, sino que aumenta el riesgo de que una de estas aplicaciones tenga una vulnerabilidad que pueda ser aprovechada por un atacante y conseguir el control del dispositivo. Por eso es recomendable desinstalar toda aplicación que no sea estrictamente necesaria para el desempeño del dispositivo, y así minimizar el riesgo de exposición por una aplicación vulnerable.

Además, es importante leer los permisos y condiciones tiene que deben ser aceptados antes de instalar una aplicación y comprobar la reputación de la misma.

5.11.5.4 Protección antivirus

Se recomienda disponer de un antivirus en el dispositivo móvil como medida extra de protección contra el malware.

5.11.5.5 Actualizaciones de software

Los sistemas operativos de los dispositivos incluyen un sistema de actualización de aplicaciones. Mediante una notificación, informan que existe una nueva versión de una aplicación instalada. Estas actualizaciones, además de añadir funcionalidades, corrigen fallos de seguridad.

Siempre que el sistema notifique de una actualización disponible, se debe aceptar y aplicar la nueva versión. Manteniendo el sistema actualizado se evitan posibles infecciones por aplicaciones vulnerables.

5.11.6 Otras Recomendaciones.

Otras recomendaciones importantes, además del sentido común a la hora de usar los dispositivos móviles y pensar siempre en lo que se está haciendo, son las siguientes:

5.11.6.1 No almacenar información sensible.

La información más delicada de la empresa u organización no debe ser almacenada en dispositivos móviles, aunque estén cifrados puesto que los dispositivos móviles suponen riesgos

5.11.6.2 WIFI públicas

Las redes inalámbricas de uso público, o compartido, como las disponibles en hoteles o cafeterías pueden suponer un riesgo.

A pesar de que tenga contraseña para poder utilizarse, un atacante podría conectarse y capturar el tráfico de todas las personas que se encuentran conectadas a esa red inalámbrica. Podría entonces analizar el tráfico capturado y recopilar contraseñas o datos confidenciales.

Si se va a hacer uso de redes inalámbricas de uso público, se recomienda no acceder a ningún servicio que requiera contraseña, realizar operaciones bancarias o descargar documentos confidenciales.

5.11.6.3 Desactivar comunicaciones inalámbricas

Es muy importante desactivar las redes inalámbricas si no se van a utilizar a corto plazo. Las redes más usuales suelen ser WIFI, Bluetooth, o infrarrojos.

Es posible realizar ataques contra redes inalámbricas, utilizando puntos de acceso falsos, y engañando al dispositivo para que se conecte automáticamente a una red de supuesta confianza. El usuario navegaría entonces sin tener constancia de que el tráfico está siendo monitoreado por un atacante.

5.11.6.4 Cargadores públicos

Se han dado casos de fugas de información en dispositivos móviles por haber sido conectados en cargadores públicos. Se debe evitar conectar el dispositivo por USB a cualquier ordenador público, como hoteles o cibercafés, y cualquier otro aparato que no tengamos total confianza en él. Pueden haber sido manipulados para extraer información de cualquier dispositivo USB al que se conecten.

5.11.7 Conclusiones.

El uso tan extendido de dispositivos móviles ha hecho que se conviertan de manera activa en una herramienta más de nuestro trabajo, alojando en muchas ocasiones información corporativa crítica o valiosa que, en caso de ser interceptada, conllevaría grandes problemas de seguridad.

Dicho uso tan extendido de estos dispositivos ha hecho que los ciberdelincuentes lo vean como un nicho de mercado a explotar, y hoy en día, los dispositivos móviles se han convertido en uno de los focos principales para ataques informáticos.

Por todo lo anterior, se recomienda la aplicación de las medidas de control implantar una estrategia de seguridad en movilidad con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información corporativa.

Es importante conocer bien las opciones que cada fabricante ofrece, y aplicar una configuración de seguridad adecuada en aras de manipular el dispositivo móvil sin perder funcionalidad.

También es importante saber qué información podemos almacenar o no en nuestro dispositivo (evitar siempre información confidencial) y qué aplicaciones (las mínimas y necesarias) y de dónde las instalamos (siempre de fuentes fiables).

6. CUMPLIMIENTO DE LAS POLÍTICAS Y PROCEDIMIENTOS

6.1. Todos los empleados deben cumplir con las Políticas de Seguridad Informática y sus documentos relacionados. Los empleados que por negligencia violen estas normas serán objeto de sanciones disciplinarias o despido.

6.2. La DGTI realizarán acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

6.3. La DGTI podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, con el fin de revisar la actividad de los procesos que ejecuta y la estructura de los archivos que se procesan.

6.4. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad Informática.

6.5. Los empleados que sean propietarios de la información deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

7. CUMPLIMIENTO DE LA LEGISLACIÓN Y NORMATIVA

Todas las Políticas de Seguridad Informática deben cumplir con la legislación aplicable, como las leyes de protección de datos, acceso a la información, protección de información personal y documentos electrónicos.