MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ELABORÓ:	REVISÓ:	APROBÓ:
OSCAR FABIAN ENCISO PEDRAZA **INGENIERO SEGURIDAD DE LA INFORMACIÓN**	ING. ATKIN ALEJANDRA TRIANA **JEFE OFICINA INFORMÁTICA**	CR. GIOVANNI RODRIGUEZ LEÓN **DIRECTOR ICFE**

TABLA DE CONTENIDO

Página

1. INTRODUCCIÓN

La gestión de seguridad de la información implica la organización y coordinación de todos los esfuerzos encaminados al aseguramiento del entorno informático del Instituto, para lo cual es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por los funcionarios y terceros del Instituto.

La Política de Seguridad de la Información es la declaración general que representa la posición de la Dirección del Instituto de Casas Fiscales del Ejército con respecto a la protección de los activos de información.

El presente documento se encuentra estructurado con una Política General de Seguridad de la Información y Políticas Específicas que soportan el Sistema de Gestión de Seguridad de la Información, las cuales deben ser conocidas y aceptadas por todos los usuarios de la infraestructura tecnológica y la información del Instituto.

2. JUSTIFICACIÓN

La Resolución No 065 del 24 de Mayo de 2016, del INSTITUTO DE CASAS FISCALES DEL EJÉRCITO, por medio de la cual se adopta la Directiva No 2014-18 del 19 de Junio de 2014 “Políticas de Seguridad de la Información para el Sector Defensa”, establece la elaboración del Manual de Seguridad de la Información para el Instituto.

3. MARCO CONCEPTUAL

Acción correctiva: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del ICFE. Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el ICFE. Ejemplo: archivo de Word “listado de personal.docx”.
- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: SAIMF.
- **Personal:** Es todo el personal del ICFE, el personal subcontratado, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del ICFE. Ejemplo: Pedro Pérez.

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a proveedores y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.
- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: Equipo de cómputo, teléfonos, impresoras.
- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Pagaduría.
- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: Un sistema de seguimiento de incidentes (denominado en inglés como issue tracking system, trouble ticket system o incident ticket system) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Los sistemas de este tipo son comúnmente usados en la central de llamadas de servicio al cliente de una organización para crear, actualizar y resolver incidentes reportados por usuarios, o inclusive incidentes reportados por otros funcionarios, contratistas, colaboradores de la entidad o de terceras partes. Un sistema de seguimiento de incidencias también contiene una base de conocimiento que contiene información de cada cliente, soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una entidad de software puede tener ambos, y algunos bugtrackers pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

Alcance: Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso. Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara. Se aplica a entidades tales como usuarios, procesos, sistemas de información.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista. De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).
Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Denegación de servicios: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Gusanos: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Ingeniería Social: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
Keyloggers: Aplicaciones que registran el teclado efectuado por un usuario.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Terceros: Personal que no tiene una vinculación directa laboralmente con la Entidad (Contratistas, pasantes, y ciudadanía en general que establece algún tipo de contacto con el Instituto)

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del ICFE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del ICFE y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. MARCO LEGAL

- Constitución Política de Colombia 1991.
- Ley 80 de 1993 “Estatuto General de contratación de la administración Publica”.
- Ley 87 de 1993 “Control interno en los organismos del Estado”.
- Ley 527 de 1999 “Comercio Electrónico”.
- Ley 594 del 2000 “Ley General de Archivo”.
- Ley 599 del 2000 “Código Penal Colombiano”.
- Ley 603 del 2000 “Control de legalidad del Software”.
- Ley 734 de 2002 “Código Disciplinario Único”.
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la Información”.
- Ley 1273 de 2009 “Protección de la Información y de los datos”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de Junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- Norma Técnica Colombiana NTC-ISO/IEC 27000
- Directiva No 2014-18 “POLIITCAS DE SEGURIDAD DE LA INFORMACION PARA EL SECTOR DEFENSA”.

5. OBJETIVO

Dar a conocer a todos los funcionarios y terceros del Instituto, las políticas y estándares que se deben cumplir para proteger y/o preservar los activos de información.

6. ALCANCE

Las Políticas definidas en el presente manual aplican a toda la entidad, empleados públicos, trabajadores oficiales, personal militar en comisión, contratistas y pasantes del INSTITUTO DE CASAS FISCALES DEL EJÉRCITO, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y Seguridad de la Información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo

un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección del Instituto.

7. REVISIÓN DE LAS POLÍTICAS

Las Políticas de Seguridad de la Información del presente manual serán revisadas anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la Política. Con el fin de asegurar que se encuentren ajustadas a los requerimientos del Instituto.

8. ROLES Y RESPONSABILIDADES

8.1. Ingeniero de Seguridad de la Información

a) Definir y establecer las políticas de seguridad de la información, alineadas con las emitidas por el Ministerio de Defensa Nacional.
b) Coordinar la implementación de las políticas de Seguridad de la Información con los diferentes procesos del Instituto.
c) Reportar a la Jefatura de Informática el estado de la Seguridad de la Información del Instituto.
d) Definir e implementar la estrategia de divulgación y concientización de Seguridad de la Información para todos los funcionarios y terceros que tengan acceso a los activos de información del Instituto.
e) Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten la labor de seguridad de la información.
f) Coordinar y ejercer control en el cumplimiento de las Políticas de Seguridad de la Información.

8.2. Funcionarios y usuarios de los sistemas de información

Todos los funcionarios del Instituto, empleados públicos, trabajadores oficiales, personal militar en comisión, contratistas y pasantes, son responsables por el cumplimiento de las Políticas de Seguridad de la Información. Adicionalmente están comprometidos a reportar por escrito al correo del Ingeniero de Seguridad de la Información cualquier evento o incidente de seguridad del que tenga conocimiento.

8.3. Administradores de los Sistemas de Información

Los administradores de los diferentes sistemas deben en forma activa implementar las medidas técnicas y procedimientos para brindar un nivel apropiado de seguridad de la información, de acuerdo a las políticas de seguridad de la información del Instituto de Casas Fiscales del Ejército.

8.4. Oficina de Control Interno

Realizar auditorías a los procesos del Sistema de Gestión de Seguridad de la Información, una vez implementado, como mínimo una vez al año.

8.5. Oficina de Contratos

Esta dependencia tiene dentro de sus funciones realizar la revisión de requisitos para proceder a la posesión como servidor público. Como parte de la función de selección se debe realizar una verificación de los antecedentes y referencias de los candidatos, garantizar que los funcionarios firmen el acuerdo de confidencialidad.

8.6. Oficina Asesora Jurídica

Esta oficina es la responsable de garantizar que se incluyan las cláusulas de confidencialidad de la información dentro de los contratos de los contratistas.

9. COMPROMISO DE LA DIRECCIÓN

La Dirección General del INSTITUTO DE CASAS FISCALES DEL EJÉRCITO aprueba este Manual de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Dirección del Instituto demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las Políticas de Seguridad de la Información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

10. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

10.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El **INSTITUTO DE CASAS FISCALES DEL EJÉRCITO ICFE** se compromete con el cumplimiento de los lineamientos del Sector Defensa, preservando los atributos de confidencialidad, integridad y disponibilidad de la información, promoviendo una cultura de seguridad y administrando los riesgos de los activos de información, mediante el establecimiento, implementación, mantenimiento y mejoramiento continuo de las políticas de seguridad de la información, contribuyendo con la misión, visión y objetivos estratégicos del Instituto.

OBJETIVOS

- Proteger los recursos de información y tecnología utilizados para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos.
- Implementar un Sistema de Gestión de Seguridad de la Información, orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información en el Instituto.

- Promover, mejorar y mantener un nivel de cultura en seguridad de la información, así como lograr la concientización de todos los funcionarios y terceros que interactúan con el Instituto, para minimizar la ocurrencia de incidentes de seguridad de la información.

10.2. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

10.2.1. POLITICA DE CLASIFICACION DE LA INFORMACION

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere el ICFE como por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información transmitida vía oral o por cualquier otro medio de comunicación.

Toda la información deberá ser identificada, clasificada y documentada.
Los usuarios responsables de la información del ICFE, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Los niveles de clasificación de la información que se han establecido son: **INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA.**

10.2.2. POLITICA DE GESTION DE ACTIVOS DE INFORMACIÓN

- Los activos de información del INSTITUTO DE CASAS FISCALES DEL EJERCITO, serán identificados, clasificados y valorados para establecer los mecanismos de protección necesarios, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información (Anexo G); así mismo tendrán un propietario asociado quien es el responsable de definir quienes tienen acceso y que pueden hacer con la información.

- Los recursos TIC que no pertenezcan al ICFE, incluidos computadores portátiles, teléfonos inteligentes, tabletas, etc. No deberán conectarse a las redes, a los sistemas ni a los servicios del ICFE (o utilizarse para obtener acceso a las aplicaciones de éste) sin la aprobación explícita del Jefe de la Oficina de Informática y tras verificar que tales recursos cumplan con los requerimientos mínimos de seguridad del ICFE (tales como software antivirus actualizado, cortafuegos habilitado, inexistencia de software de escaneo de redes u otros programas objetables). Lo anterior debido a que los dispositivos de comunicación personal (teléfonos inteligentes y tabletas) que se conecten a la red inalámbrica de la oficina, a los sistemas o a los servicios de la Entidad representan un riesgo para la Seguridad de la Información y una carga adicional a la conexión de Internet, ya que dichos dispositivos están normalmente conectados a cuentas personales de redes sociales u otros servicios.
- Todos los servidores públicos y terceros que utilicen los recursos TIC deben seguir las políticas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, establecidos por la Entidad.

- Se deben emplear medidas de protección para el cableado de la red y dispositivos de comunicación de manera que no se exhiban ni sean de fácil acceso generando el riesgo de conexiones no autorizadas.

- Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los equipos que contengan medios de almacenamiento y que serán reutilizados o eliminados, con el fin de garantizar que la información de la Entidad contenida en estos medios no se pueda recuperar.

- Los recursos de red que ha dispuesto el ICFE, tales como carpetas compartidas, no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, ejemplos de información no permitida son: Material pornográfico, videos, películas, música, fotos, etc.

10.2.2.1 ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

A continuación se describen algunas acciones identificadas que afectan la seguridad de la información y que, al poner en riesgo la disponibilidad, confidencialidad e integridad de la misma, se deben evitar:

a. Dejar los computadores encendidos en horas no laborales.
b. Permitir que personas ajenas al ICFE ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
c. No clasificar y/o etiquetar la información.
d. No guardar bajo llave documentos impresos que contengan información clasificada, al terminar la jornada laboral.
e. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
f. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
g. Hacer uso de la red de datos del ICFE, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
h. Instalar software en la plataforma tecnológica del ICFE, cuyo uso no esté autorizado por la Oficina de Informática, atentando contra las leyes de derechos de autor o propiedad intelectual.
i. Destruir la documentación institucional, sin seguir los parámetros y normatividad vigente establecida para el proceso de gestión documental.
j. Descuidar información clasificada del ICFE, sin las medidas apropiadas de seguridad que garanticen su protección.
k. Enviar información no publica por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
l. Almacenar y mantener información clasificada en dispositivos de almacenamiento de cualquier tipo que no sean de propiedad del ICFE.
m. Conectar computadores portátiles u otros dispositivos electrónicos personales, a la red de datos del ICFE, sin la debida autorización de la Oficina de Informática.
n. Ingresar a la red de datos del ICFE, por cualquier servicio de acceso remoto, sin la autorización de la oficina de Informática.
o. Usar servicios de internet en los equipos del Instituto, diferente al provisto por la oficina de informática del ICFE.

p. Promover o mantener actividades personales utilizando los recursos tecnológicos del ICFE, para beneficio personal.
q. Uso de la cuenta y contraseña de otro usuario, o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.
r. Descuidar dejando al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
s. Retirar de las instalaciones del ICFE, computadores de escritorio, portátiles e información clasificada, física o digital sin autorización, o abandonarla en lugares públicos o de fácil acceso.
t. Entregar, enseñar o divulgar información clasificada del ICFE a personas o entidades no autorizadas.
u. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica del ICFE.
v. Ejecutar cualquier acción que difame, afecte la reputación o imagen del ICFE, o alguno de sus servidores públicos, utilizando para ello la plataforma tecnológica.
w. Realizar cambios no autorizados en la plataforma tecnológica del ICFE.
x. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
y. Ejecutar acciones para eludir y/o modificar los controles establecidos en el presente manual.
z. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la seguridad de la información, acarrearan medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

10.2.3. POLITICA DE GESTION DE TERCEROS

a) Cuando exista la necesidad de otorgar acceso de terceras partes al ICFE, deberá realizarse siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre los siguientes aspectos:

- El tipo de acceso requerido (Físico, lógico y a que recurso).
- Los motivos para los cuales solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.

b) En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones del ICFE, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.

c) En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicio críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

d) El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la oficina de Informática, aprobarán y autorizaran el acceso y uso de la información.

e) Los contratos o acuerdo de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplaran como mínimo los siguientes aspectos:

- Forma en los que se cumplirán los requisitos legales aplicables.
- Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas conocen sus responsabilidades en materia de seguridad.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
- Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
- Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
- Niveles de seguridad física que se asignará al equipamiento tercerizado.
- Derecho a la auditoria por parte del ICFE.

10.2.4. POLITICA DE ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados públicos y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos, utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

10.2.5. POLITICA DE ACUERDO DE INTERCAMBIO DE INFORMACION Y SOFTWARE

a) Todo empleado público y/o tercero es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

b) Los propietarios de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de acuerdo a la documentación vigente.

c) El intercambio de información y de software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen cláusulas de responsabilidad, deberes y derechos.
d) Los acuerdos de intercambio, deben en todo caso velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo deben especificar las consideraciones de seguridad y reserva de la información, y las responsabilidades por el mal uso o divulgación de la misma.

e) Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realizará siguiendo el procedimiento establecido por la entidad que solicita la información.

f) El intercambio de información deberá contemplar las siguientes directrices:
- Uso de WebServices, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.
- Respeto por los derechos de autor del software intercambiado.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
- Informar al titular de los datos, el intercambio de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

10.2.6. POLITICA DE USO DE INTERNET

a) La navegación en internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se consideraran aceptables los siguientes usos:

1. Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

2. Publicación, envío o adquisición de material sexualmente explicito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.

3. Publicación o envío de información confidencial hacia afuera del ICFE sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

4. Utilización de otros servicios disponibles a través de internet que permitan establecer conexiones o intercambios no autorizados.

5. Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.

6. Promover o mantener asuntos o negocios personales.

7. Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.

8. Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte del Instituto.

9. Uso de herramientas de mensajería instantánea no autorizadas por la oficina de informática.

10. Emplear cuentas de correo externas, no corporativas, para el envío o recepción de información institucional.

b) Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los empleados públicos y terceros autorizados. Así mismo, se pueden inspeccionar, registrar o informar las actividades realizadas durante la navegación.

c) El uso de internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

10.2.7. POLITICA DE USO DE CORREO ELECTRONICO INSTITUCIONAL O CORPORATIVO

a) La cuenta de correo electrónico institucional debe ser usada únicamente para el desempeño de las funciones asignadas por el ICFE.

b) Los mensajes y la información contenida en los buzones de correo institucional son de propiedad del ICFE. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo, la información y el tráfico de la misma, se considera de interés del sector Defensa.

c) El tamaño de los buzones y mensajes de correo serán determinados por la oficina de Informática del ICFE, conforme a las necesidades de cada usuario y previa autorización del jefe inmediato.

d) Se debe suministrar una cuenta de correo corporativa por cada oficina que lo requiera, la cual será utilizada para el envío masivo de correos institucionales.

e) No se considera aceptado el uso del correo electrónico corporativo para los siguientes fines:

1. Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales, incluido el lavado de activos.

2. El envío de cualquier tipo de archivo que ponga en riesgo la seguridad de la información; en caso que sea necesario hacer un envío de este tipo de archivos, deberá contar con la autorización correspondiente por parte de la oficina de Informática.

3. El envío de información relacionada con la defensa y la seguridad nacional a otras entidades del gobierno diferentes a las que conforman el Sector Defensa, sin la autorización previa del propietario de la información y de la oficina de Informática.

f) Toda información que requiera ser transmitida fuera del ICFE, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. Solo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

g) Todo correo electrónico deberá respetar el estándar de formato e imagen corporativa definido para el ICFE, y deberá contener al final del mensaje, un texto en español e inglés en el que se contemplen mínimo los siguientes elementos:

1. El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la ley.

2. El mensaje solo puede ser utilizado por la persona o empresa a la cual está dirigido.

3. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

4. Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

h) No es permitido en ningún caso, accesar ni compartir mensajes de correos con información en archivos adjuntos de dudosa procedencia. Si se recibe un correo de origen desconocido, se debe consultar inmediatamente con el Ingeniero de Seguridad de la Informacion. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos de correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keylogger, gusanos, etc).

10.2.8. POLITICA DE USO DE REDES INALAMBRICAS

a) Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a la red Institucional.

b) Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado entre otros.

c) Se debe implementar infraestructura inalámbrica que permita configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas establecidas por defecto.

10.2.9. POLITICA DE SEGREGACION DE REDES

a) La plataforma tecnológica del ICFE que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos, e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet.

b) La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si asi se requiere. La oficina de Informática es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

10.2.10. POLITICA DE COMPUTACION EN LA NUBE (CLOUD COMPUTING)

a) Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos.

b) Ningún servicio de carácter operativo e institucional del ICFE deberá ser contratado en servicios en la nube público o hibrido.

c) Se podrá implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

10.2.11. POLITICA DE SISTEMAS DE INFORMACIÓN DE ACCESO PÚBLICO

a) La información pública producida por el ICFE deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

b) Todo portal Institucional deberá contener la política de privacidad y uso, asi como la política de seguridad del mismo.

c) El ICFE deberá garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales, y propender por la seguridad de la información ingresada a través de ellos, aclarando que no es responsable de la veracidad de la misma.

10.2.12. POLITICA DE RECURSOS TECNOLOGICOS

a) La instalación de cualquier tipo de software en los equipos de cómputo del ICFE, es responsabilidad exclusiva de la oficina de Informática, por tanto son los únicos autorizados para realizar esta labor.

b) Ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.

c) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la oficina de Informática del ICFE.

d) Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como cambio de ubicación, mantenimiento, repotenciación y modificaciones en su configuración física. Estas actividades solo podrán ser realizadas por la oficina de Informática del ICFE.

e) Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable, una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación con el ICFE.

f) De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas, una vez se haya cesado el uso de los mismos.

10.2.13. POLITICA DE CONCIENTIZACION Y CAPACITACION EN SEGURIDAD DE LA INFORMACION

a) Se debe mantener un programa anual de concientización y capacitación para todos sus funcionarios, así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades dentro del Instituto.

b) Todos los funcionarios y terceros al servicio del ICFE, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

10.2.14. POLITICA DE FINALIZACION DE LA RELACION LABORAL

Al momento de la desvinculación o de cambio de roles, todo funcionario y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados. Esto mediante un formato establecido por la oficina de Informática del ICFE.

10.2.15. POLITICA DE SEGURIDAD FISICA

a) Se consideran áreas de acceso restringido a todas las áreas donde se encuentran alojados los equipos de procesamiento o almacenamiento de información privada, la infraestructura de soporte a los sistemas de información y comunicaciones, y las áreas donde se encuentra la documentación privada del ICFE; por lo cual se deben emplear mecanismos de acceso físico que garanticen que sólo se permite el acceso al personal autorizado.

b) Las áreas de acceso restringido deben contar con mecanismos efectivos que permitan cumplir con los requerimientos ambientales de temperatura y humedad especificados por los fabricantes de los equipos que albergan, y conservación de la documentación que custodia, además de medidas para proteger los equipos del polvo y prevenir amenazas externas como manifestaciones sociales, explosiones en la calle o vandalismo.

c) El acceso a las áreas restringidas por parte del personal de soporte técnico de proveedores se debe otorgar y monitorear, únicamente cuando sea necesario por medio de una autorización.

d) Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados, evitar que las puertas se dejen abiertas.

e) No está permitida la toma de fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen del Instituto, a menos que esté autorizado.

f) Todos los funcionarios y contratistas deben portar en un lugar visible el carnet que los identifica como funcionarios o contratistas del Instituto, para el acceso a la Entidad y mientras se encuentre dentro de ella.

g) Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.

h) Los funcionarios se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a equipos de cómputo, tales como: impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipos que generen caídas de la energía.
i) Es responsabilidad de todos los funcionarios y terceros, acatar las normas de seguridad y mecanismos de control de acceso al Instituto.

j) Los funcionarios y terceros, así como los visitantes, deberán tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones del ICFE.

k) Los funcionarios y terceros no deben consumir alimentos ni bebidas en las áreas donde se encuentren activos de información.

l) Todos los escritorios o mesas de trabajo deben permanecer ordenados y asegurados con el fin de no exponer elementos con información crítica tales como documentos físicos y dispositivos de almacenamiento ante visitantes mal intencionados y de esta forma reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

10.2.16. POLITICA DE SEGURIDAD Y MANTENIMIENTO DE LOS EQUIPOS

a) Los equipos que hacen parte de la infraestructura tecnológica del ICFE deben ser ubicados y protegidos adecuadamente para prevenir la perdida, daño, robo o acceso no autorizado de los mismos.

b) Se adoptarán los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

c) Los funcionarios y terceros velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

d) Se debe asegurar que sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos, con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, se revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

e) Los equipos tales, como máquinas de copiado, impresoras y máquinas de fax, deberán estar ubicados en zonas de acceso restringido, y se permitirá el uso únicamente a personal autorizado.
f) Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones del ICFE.

g) Se debe garantizar la existencia de polizas o seguros para la reposicion de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

10.2.17. POLITICA DE SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

a) Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones del ICFE, deben velar por la protección de los mismos, sin dejarlos desatendidos, comprometiendo la imagen o información del Instituto.

b) El propietario del activo, con el apoyo de la oficina de Informática, identificará mediante una tecnología de análisis de riesgos; las vulnerabilidades potenciales que puede generar el retiro de equipos o medios, de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

c) En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la defensa y la seguridad nacional, se deberá realizar inmediatamente el respectivo reporte, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo F), y se deberá poner la denuncia ante la autoridad competente, si aplica.

d) Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones del ICFE, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o que puedan poner en riesgo la información que contiene.

10.2.18. POLITICA DE TRASLADO DE PROPIEDAD

a) El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica del ICFE, debe ser autorizado por el propietario del activo, previa solicitud del funcionario interesado.

b) Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones del ICFE, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.

c) Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos del ICFE, solo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a través del proceso de sanitizacion. La oficina de Informática generará un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas del Instituto.

10.2.19. POLITICA DE PROTECCION CONTRA SOFTWARE MALICIOSO

a) Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en los procedimientos de Gestión de Vulnerabilidades Técnicas (Anexo J) y Control de Cambios (Anexo H).
b) Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas de software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

c) Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la oficina de Informática; y deberán ser actualizados periódicamente.

d) No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación, diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

e) Todos los medios de almacenamiento que se conecten a equipos de la infraestructura tecnológica del ICFE, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

f) La oficina de Informática será responsable de que los usuarios del ICFE mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

g) Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

10.2.20. POLITICA DE COPIAS DE RESPALDO

a) Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la oficina de Informática y las dependencias responsables de la misma, contenida en la plataforma tecnológica del ICFE, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el Procedimiento de Gestión de copias de respaldo y recuperación (Anexo K).

b) Los medios de las copias de respaldo se almacenarán tanto localmente como en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

c) Se deberá establecer un plan de restauración de copias de seguridad que será probado a intervalos regulares, establecidos según las necesidades y capacidades del Instituto, con el fin de asegurar que son confiables en caso de emergencia. Estas copias serán retenidas por un periodo de tiempo determinado, de acuerdo a lo establecido en el procedimiento de Gestión de copias de respaldo (Anexo K).

d) La oficina de Informática del ICFE, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca de su traslado, frecuencia e identificación; así mismo, definirá conjuntamente con las dependencias usuarias los periodos de retención de dicha información.

e) Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

10.2.21. POLITICA DE GESTION DE MEDIOS REMOVIBLES

a) Se restringe la conexión no autorizada a la infraestructura tecnológica del ICFE, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

b) Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos.

c) La oficina de Informática, con debida autorización del Director del ICFE definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser requerido para el cumplimiento de sus funciones.

d) Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene, dando cumplimiento a los lineamientos establecidos en el procedimiento de Inventario y Clasificación de Activos de Información (Anexo G). Si un medio removible llegase a contener información con distintos niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.

e) Para los procesos de baja, de reutilización o de garantía de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. La destrucción segura se documentará mediante acta, registro fílmico y fotográfico.

f) El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario de dicho activo.

10.2.22. POLITICA DE COMPUTACION MOVIL

a) Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se debe implementar controles de acceso y técnicas criptográficas para cifrar la información crítica almacenada en estos.

b) La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser debidamente autorizada por la oficina de Informática, previa verificación de que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura.

10.2.23. POLITICA DE GESTION DE REGISTROS

a) Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento de red y de seguridad informática, deberán generar registros de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento Monitoreo y Revisión de Logs (Anexo L).

b) El tiempo de retención de los Logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.

c) El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

d) Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la oficina de Informática, mediante el procedimiento de Gestión de Incidentes de Seguridad (Anexo F).

10.2.24. POLITICA DE CONTROL DE ACCESO

a) Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

b) El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el propietario de cada activo, según el procedimiento de Gestión de Usuarios y Contraseñas (Anexo M).

c) Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad Informática del ICFE deberá estar autorizado por la oficina de Informática.

d) Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso, el tráfico de datos deberá estar cifrado.

e) La creación, modificación, y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática deberá seguir el procedimiento Gestión de usuarios y Contraseñas (Anexo M).

f) Todo usuario que se cree para que un tercero ingrese a la red del ICFE, debe tener una fecha de vencimiento específica, la cual en ningún caso debe superar la fecha de terminación de sus obligaciones contractuales.

g) La asignación de privilegios en las aplicaciones para los diferentes usuarios estarán determinados por el procedimiento Gestión de Usuarios y contraseñas (Anexo M). Estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

h) Los equipos de terceros que requieren acceder a la red del ICFE, deben cumplir un procedimiento de sanitizacion informática antes de concedérseles dicho acceso.

10.2.25. POLITICA DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

a) No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

b) La oficina de Informática debe garantizar que el control de acceso al centro de datos del ICFE, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

c) La oficina de Informática deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

d) La limpieza y aseo del centro de datos estará a cargo de la oficina de Informática. Esta labor no será realizada por ninguna otra persona ajena a esta dependencia, con el fin de evitar alguna desconexión en los servicios.

e) En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

f) El centro de datos debe estar provisto de:
   - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
   - Pisos elaborados con materiales no combustibles.
   - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
   - Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
   - Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
   - Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

g) El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
h) Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

i) La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por la oficina de Informática y exclusivamente con fines institucionales.

j) Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del ICFE.

k) Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

l) Cuando se requiera realizar alguna actividad sobre algún armario (*rack*), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

m) Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

n) Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

10.2.26. POLITICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESION

a) Los documentos que se impriman en las impresoras del ICFE deben ser de carácter institucional, por ningún motivo se deben realizar impresiones u otro servicio de carácter personal.

b) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

c) Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la oficina de Informática.

10.2.27. POLITICA DE UNIDADES DE RED Y CARPETAS VIRTUALES

a) Para que los usuarios tengan acceso a la información ubicada en las unidades de red o carpetas virtuales, el jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la oficina de Informática del ICFE. Los usuarios tendrán permisos de escritura, lectura o modificación de información en las unidades de red, dependiendo de sus funciones y su rol.

b) La información almacenada en cualquiera de las unidades de red o carpetas virtuales debe ser de carácter institucional.

c) Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en las unidades de red o carpetas virtuales.

d) Se prohíbe extraer, divulgar o publicar información de cualquiera de las unidades de red, carpetas virtuales o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

e) Se prohíbe el uso de la información de las unidades de red o carpetas virtuales con fines publicitarios, de imagen negativa, lucrativa o comercial.

10.2.28. POLITICA DE ADMINISTRACION DE CONTRASEÑAS

a) La administración, así como la asignación y entrega de las contraseñas a los usuarios deberá seguir el procedimiento Gestión de Usuarios y Contraseñas (Anexo M).

b) Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

1. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
2. Las contraseñas no deberán ser reveladas.
3. Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento Gestión de Usuarios y Contraseñas (Anexo M).
4. Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que una persona esté utilizando un usuario y contraseña que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo F).

10.2.29. POLITICA DE BLOQUEO DE SESION, ESCRITORIO Y PANTALLA LIMPIA

a) En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica, protegida bajo llave.
b) Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

c) Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por el Instituto.

d) Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo, documentos, acceso directos a los mismos o a sistemas de información sensibles.

e) Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

10.2.30. POLITICA DE CONTROLES CRIPTOGRAFICOS

a) Se deben identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento de Inventario y Clasificación de Activos de Información (Anexo G), tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

b) No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la oficina de Informática, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y terceros autorizados.

10.2.31. POLITICA DE GESTION DE VULNERABILIDADES TECNICAS

a) La oficina de informática se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

b) La oficina de Informática será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica del Instituto.

c) No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la oficina de Informática, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del ICFE, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

d) Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.
e) Se realizará por parte del área competente, el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

f) La oficina de Informática realizará las revisiones de las alertas de seguridad, definiendo en caso de ser necesario, un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

10.2.32. POLITICA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

a) Los funcionarios y terceros deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo F).

b) Para los casos en que los incidentes reportados requieran judicialización, se deberá coordinar con los organismos que cuentan con función de policía judicial.

c) Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad (Anexo F) para la Institución.

d) Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo, y de ser posible, la valoración de los daños.

e) Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

f) Los resultados de las investigaciones que involucren a los funcionarios del ICFE deberán ser informados a las áreas de competencia.

g) La oficina de Informática deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

10.2.33. POLITICA DE SEGURIDAD DE LA INFORMACION EN LA CONTINUIDAD DELNEGOCIO

a) La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

b) El Instituto debe contar con un plan de Continuidad del Negocio que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

c) Para el ICFE, su activo más importante es el recurso humano, y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.
d) Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio.

e) Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.

10.2.34. POLITICA DE DOCUMENTACION DE PROCEDIMIENTOS OPERATIVOS

a) La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

b) Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contacto de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

c) La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por el administrador de la aplicación, propietario del activo, jefe de dependencia o el funcionario a quien se le hayan otorgado dichas funciones.

d) Los procedimientos operativos deben contener instrucciones para el manejo de los errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

10.2.35. POLITICA DE CONTROL DE CAMBIOS OPERATIVOS

a) Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la oficina de Informática, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

b) Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de Control de Cambios (Anexo H). Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

10.2.36. POLITICA DE SEGREGACION DE FUNCIONES

a) Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, deben contar con una definición clara de los roles y funciones sobre estos, para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

b) La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por la oficina de Informática, con el fin de mantener actualizada dicha información acorde con la realidad del ICFE.

10.2.37. POLITICA DE SEPARACION DE AMBIENTES

a) El ICFE proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

b) El paso de software y hardware, de un ambiente a otro, deberá ser controlado y gestionado de acuerdo con lo definido en el procedimiento de Control de Cambios (Anexo H).

c) Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción, así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

d) No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

e) El ambiente del sistema de prueba debe emular el ambiente de producción, lo más estrechamente posible.

f) No se permite la copia de Información Ultra Secreta, Reservada, Confidencial, Restringida o Exclusiva, desde el ambiente de producción al ambiente de pruebas; en caso de ser estrictamente necesario, la copia debe contar con las respectivas autorizaciones y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y que se elimine de forma segura después de su uso.

g) Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

h) Periódicamente se deberá verificar las versiones instaladas tanto en ambiente de pruebas como en producción y se confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de cada institución y entidad del sector.

10.2.38. POLITICA DE CONTROL DE VERSIONES

a) Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma, de acuerdo con el procedimiento de Control de Versiones (Anexo O).

b) El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.

c) Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde solo se permita el acceso al personal autorizado.

d) Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo F).

10.2.39. POLITICA DE GESTION DE LA CAPACIDAD

a) La oficina de Informática, como área responsable de la administración de la plataforma tecnológica, deberá implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación, conforme a lo establecido en el procedimiento de Gestión de la Capacidad (Anexo I).

10.2.40. POLITICA DE DERECHOS DE PROPIEDAD INTELECTUAL

a) El ICFE cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementará los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

b) No se permitirá el almacenamiento, descarga de internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

c) Se permitirá el uso de documentos, cifras y/o textos de carácter público, siempre y cuando se cite el autor de los mismos, con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

d) Los procesos de adquisición de aplicaciones y paquetes de software, cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

e) El software a la medida, adquirido a terceras partes o desarrollado por funcionarios del ICFE, serán de uso exclusivo del Instituto y la propiedad intelectual será de quien lo desarrolle.

11. SANCIONES PARA LAS VIOLACIONES A LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores del ICFE. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

A continuación se relacionan las definiciones de delitos informáticos, y los artículos que las respaldan.

11.1. DELITOS INFORMATICOS

Delitos informáticos" son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático. El Delito Informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de los computadores es lo que ha propiciado la necesidad de regulación por parte del derecho.

Dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Un incidente representa un reto para demostrar la diligencia de su organización para enfrentar el hecho, tomar el control, recoger y analizar la evidencia, y finalmente generar el reporte sobre lo ocurrido, que incluye las recomendaciones de seguridad y conceptos sobre los hechos del incidente.

Por esta razón se han definido como delitos informáticos los siguientes:

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
  - Acceso ilícito a sistemas informáticos.
  - Interceptación ilícita de datos informáticos.
  - Interferencia en el funcionamiento de un sistema informático.
  - Abuso de dispositivos que faciliten la comisión de delitos.

  Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

- **Delitos informáticos:**
  - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

- **Delitos relacionados con el contenido:**
  - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:** Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Y según el código penal se estipulan los siguientes:

- **Ataques que se producen contra el derecho a la intimidad:** Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:** Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

- **Falsedades:** Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.(Artículos 386 y ss. del Código Penal)

- **Sabotajes informáticos:** Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

- **Fraudes informáticos:** Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

- **Amenazas:** Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

- **Calumnias e injurias:** Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

- **Pornografía infantil:** Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)

- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189)

- El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (art 189)

- La posesión de dicho material para la realización de dichas conductas. (art 189)

Y la Ley 1273 de 2009 se adiciona los siguientes:

- **ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **ARTÍCULO 269D: DAÑO INFORMÁTICO.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
- **ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a

su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave, la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- **ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA:** Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
  1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
  2. Por servidor público en ejercicio de sus funciones.
  3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
  5. Obteniendo provecho para sí o para un tercero.
  6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
  7. Utilizando como instrumento a un tercero de buena fe.
  8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

- **ARTÍCULO 2691: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES.** El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

12. DOCUMENTOS RELACIONADOS

TIPO			NOMBRE	CÓDIGO
P	D	F		
☐	☐	☑	FORMATO DE INVENTARIOS DE ACTIVOS DE INFORMACIÓN	ICFE-M-10 F-01
☐	☐	☑	FORMATO ACUERDO DE CONFIDENCIALIDAD	
☐	☐	☑	FORMATO AUTORIZACION INGRESO/SALIDA – EQUIPOS INSTITUCIONALES	
☐	☐	☑	FORMATO AUTORIZACION INGRESO/SALIDA – EQUIPOS ENTIDADES EXTERNAS	
☐	☐	☑	FORMATO REPORTE INCIDENTES DE SEGURIDAD	
☑	☐	☐	PROCEDIMIENTO PARA LA GESTION DE INCIDENTES DE SEGURIDAD	

TIPO			NOMBRE	CÓDIGO
P	D	F		
☑	☐	☐	PROCEDIMIENTO DE INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACION	
☑	☐	☐	PROCEDIMIENTO DE CONTROL DE CAMBIOS	
☑	☐	☐	PROCEDIMIENTO DE GESTION DE LA CAPACIDAD	
☑	☐	☐	PROCEDIMIENTO DE GESTION DE LAS VULNERABILIDADES TECNICAS	
☑	☐	☐	PROCEDIMIENTO GESTION DE COPIAS DE RESPALDO	
☑	☐	☐	PROCEDIMIENTO MONITOREO Y REVISION DE LOGS	
☑	☐	☐	PROCEDIMIENTO GESTION DE USUARIOS Y CONTRASEÑAS	
☑	☐	☐	PROCEDIMIENTO DE SANITIZACION INFORMATICA	
P: PROCEDIMIENTO O PROGRAMA **D**: DOCUMENTO **F**: FORMATO				