



**Comisión  
Federal de  
Telecomunicaciones**



## COMISIÓN FEDERAL DE TELECOMUNICACIONES

# GUÍA DE RESPONSABILIDADES DE EMPLEADOS – SEGURIDAD DE LA INFORMACIÓN

48

Control de cambios.						
Versión	Elaborado por:	Revisado por:	Autorizado por:	Fecha de revisión:	Fecha de Aplicación:	Comentarios
1.0	Miguel Ángel Zires Magaña Enrique Carrillo Díaz Mauro Paredes Noda	Guillermo Rodríguez Contreras	Rodrigo A. Gutiérrez Sandez	19/09/2008	19/09/2008	Creación del documento
2.0	Francisco Rugama Mejía	Andrés Falcón García Guillermo Rodríguez Contreras Cesar Vicente Pérez Gaytán	Rodrigo A. Gutiérrez Sandez	05/12/2008	18/02/2009	Se actualizó

Control de copias.			
Versión:	2.0		
Copia Asignada a:			
Dueño del documento:			

Handwritten marks and signatures in blue ink at the bottom of the page.

## 1 Tabla de contenido

1	TABLA DE CONTENIDO.....	2
2	PROPÓSITO Y ALCANCE.....	3
3	DEFINICIONES.....	3
4	RESPONSABILIDADES DEL USUARIO.....	5
4.1	USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN.....	5
4.2	USO DE CONTRASEÑAS.....	7
4.3	USO DE INTERNET.....	9
4.4	USO DE CORREO ELECTRÓNICO.....	10
4.5	IMPRESIÓN DE DOCUMENTOS.....	12
4.6	ENTRADA Y SALIDA DE EQUIPO DE CÓMPUTO.....	12
4.7	ENTRENAMIENTO Y CONCIENTIZACIÓN.....	13
4.8	MONITOREO DE USUARIOS.....	13
4.9	VIRUS Y CÓDIGO MALICIOSO.....	13
4.10	HERRAMIENTAS DE HACKEO INFORMÁTICO.....	14
4.11	CONTENIDO PORNOGRÁFICO.....	14
4.12	RESPALDOS DE PC'S PERSONALES.....	15
4.13	USO DE MEDIOS REMOVIBLES.....	15
4.14	SANCIONES.....	15

## 2 Propósito y alcance

### **Propósito:**

Definir las responsabilidades de los empleados de la COFETEL en el manejo y utilización de servicios y activos de la información durante la ejecución de sus funciones, a fin de cumplir con los requerimientos de seguridad y de control establecidos por la misma institución.

### **Alcance:**

Esta guía es aplicable a todos los empleados de la COFETEL que tengan acceso a cualquier servicio y activo de la información de la misma.

Esta condición será extensiva para cualquier persona externa que de igual forma accede a dichos activos o servicios informáticos propiedad de la institución, ya sea por cuestiones de trabajo o por motivos de consulta.

## 3 Definiciones

**Grupo de Seguridad Informática (GSI):** Grupo conformado por miembros de la coordinación general de organización y tecnologías de la información de la COFETEL con las funciones de analizar, definir, implementar, revisar y supervisar las políticas de seguridad informática dentro de la institución.

**Usuario:** Cualquier empleado de la COFETEL o persona que haga uso de activos o servicios de información de la institución, para el desempeño de sus funciones o por motivos de consulta

**Activos de Información:** Los activos son cualquier recurso del sistema de información o relacionado con este, que son necesarios para el desempeño de las funciones de los usuarios.

La consulta, registro, procesamiento, o transmisión de información (como la documentación digital o escrita, y la administración de la misma, como por ejemplo las bases de datos), ya sea por medio de Internet, equipo de cómputo, equipo de comunicaciones, software, medios removibles, no removibles, dispositivos externos al equipo, etc.; utilizando medios propiedad de la Cofetel, pertenecerá a la propia institución.

**Servicios Informativos:** Bienes intangibles que se proporcionan para satisfacer las necesidades de los usuarios, tales como la atención personalizada (soporte técnico, mantenimiento, asesoría, etc.), la interconexión a redes (conexión a Internet, bases de datos, servicios de impresión, etc.), y el desarrollo e implementación de aplicaciones de software.

**Medios de almacenamiento removibles:** Cualquier medio externo al equipo de cómputo en el que se almacene información incluyendo: disquetes, CD-ROM, DVD, unidades de

memoria (USB, flash, etc.), cartuchos de respaldo, unidades jazz o zip, discos duros externos, etc.

**Medios de almacenamiento no removibles:** Cualquier medio incorporado dentro de los sistemas de cómputo que almacene información, (ej.: discos duros).

**Derechos de autor:** Protección legal que cubre las actividades y trabajos de creación de productos de cualquier tipo que sean plasmados de forma tangible o material. Las leyes de derechos de autor garantizan al creador el derecho exclusivo de reproducir, preparar trabajos derivados, distribuir o mostrar el trabajo públicamente.

**Derecho de propiedad:** Protección legal destinada a proteger las invenciones individuales e industriales y que prohíben la copia, venta, reproducción o importación de determinado producto sin autorización explícita. Estos derechos pueden aplicarse a la información si ésta se aplica a la manufactura de un producto singular y utilizado para fines comerciales y de negocios. Entre las formas de propiedad intelectual existentes se tienen: patentes, marcas comerciales y de servicios, y secretos industriales y comerciales. Bajo estas consideraciones, al utilizar medios propiedad de la Cofetel, la información generado por estos pertenecerá invariablemente a la propia institución.

**Derechos de uso:** Extensión de los anteriores derechos mediante el cual el dueño de la autoría y/o propiedad moral, material o intelectual; cede los derechos parciales o totales de uso, a través de un esquema de licenciamiento o acuerdo legal.

**Software corporativo:** Software con licenciamiento de uso y/o propietario. Este software será analizado, evaluado, autorizado e instalado por el Grupo de Seguridad Informática (GSI) en los equipos pertenecientes a la COFETEL, y utilizado por empleados y proveedores para el desempeño de sus actividades y/o funciones.

**Freeware/shareware:** Software gratuito proveniente de Internet o cualquier otro medio (ej.: cursos, revistas, etc.) que no requiere la compra de una licencia para su uso, y que normalmente esta limitado en su funcionamiento bajo restricciones de uso o por períodos de tiempo. Este tipo de software requiere la autorización de instalación y uso por parte del Grupo de Seguridad Informática.

**Mecanismos de encriptación:** Técnicas bajo las cuales se transforma la información (de texto claro a texto secreto) y que solo puede ser descifrado si se cuenta con las llaves o contraseñas para dicho fin.

**Firmas digitales:** Es un conjunto de datos que incluyen códigos o algoritmos de encriptación de llave pública, en forma electrónica, que se asocian a un documento electrónico y que permite identificar a su autor y garantizar la no-repudiación así como la integridad de la información.

PS

## 4 Responsabilidades del usuario.

### 4.1 Uso aceptable de los activos de información.

- 4.1.1 El desconocimiento de estos lineamientos no es excusa para su incumplimiento.
- 4.1.2 Los usuarios son los únicos responsables del uso, protección y custodia de los activos de información que les sean asignados para el desempeño de sus funciones.
- 4.1.3 Bajo ninguna circunstancia los usuarios pueden alterar la configuración de los programas precargados (software corporativo) en los equipos de cómputo asignados, asimismo, este software no podrá ser copiados a ningún otro medio. De igual modo, esta condición es extensiva sobre la configuración física original de los equipos de cómputo dotado.
- 4.1.4 Los usuarios que tengan equipo de cómputo asignado, son los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que deben evitar compartirlos, cumpliendo con los requerimientos de seguridad física e informática establecidos en estos lineamientos. En caso de requerir compartir o prestar el equipo de cómputo o alguna información, deberá solicitar el apoyo al GSI o a la Dirección de Sistemas Informativos (vía mesa de ayuda) y sustentar el motivo de dicha petición. Estas dos instancias analizarán el impacto de dicha petición y decidirá si es procedente y los pasos consecuentes de dicha resolución.
- 4.1.5 Los usuarios tienen la responsabilidad y la obligación de revisar que todos los medios de almacenamiento removibles que sean introducidos o conectados a sus equipos de cómputo sean analizados utilizando el programa antivirus instalado por el Grupo de Seguridad Informática, esto con el fin de minimizar cualquier problema que pudiera surgir por virus, códigos o programas maliciosos.
- 4.1.6 Los usuarios tienen prohibido utilizar los activos de información para fines personales y/o de lucro.
- 4.1.7 El uso de software de apoyo laboral y de tipo personal, freeware y shareware, proveniente de Internet u obtenido a través de otro medio ajeno a la COFETEL, debe ser sujeto de un proceso de evaluación y aprobación formal para su instalación y utilización, por parte del Grupo de Seguridad Informática.
- 4.1.8 Los usuarios tienen estrictamente prohibido introducir o instalar programas o códigos destructivos o maliciosos (ej.: virus, gusanos, caballos de Troya, puertas traseras, spyware y en general, herramientas de hacking o monitoreo) de forma voluntaria o involuntaria, que puedan causar daños, interferencias con otros sistemas, accesos no autorizados o que provoquen alguna alteración en el desempeño de los activos o servicios informativos proporcionados de la COFETEL.

- 4.1.9 Los usuarios no deben utilizar los activos informativos para almacenar, reproducir, ejecutar, intercambiar, ni transmitir copias no autorizadas de software o información digital (esto incluye archivos de incluyendo audio, video y juegos) en los recursos de computo que les fueron asignados.
- 4.1.10 Los usuarios tienen prohibido utilizar los activos de información propiedad de la COFETEL para almacenar, procesar, descargar o transmitir información (ej.: cadenas de correo electrónico) con la finalidad de promover propaganda política, social, religiosa o creencias personales ajenas al desempeño de sus funciones/atribuciones.
- 4.1.11 Los usuarios tienen prohibido publicar información difamatoria o privada de alguna persona u organización sin su consentimiento, con o sin el fin de inflingirle algún daño emocional, profesional, económico o de cualquier otra índole.
- 4.1.12 Los usuarios tienen prohibido distribuir fuera de la COFETEL o en cualquier lugar forma o manera, artículos, documentos o cualquier otro material o información que sea de su propiedad intelectual o de cualquier otra índole, que haya sido clasificada como de uso interno o confidencial (ej.: manuales de políticas y procedimientos, planes estratégicos, documentación de procesos, entre otros).
- 4.1.13 Los usuarios tienen la responsabilidad de notificar inmediatamente al Grupo de Seguridad Informática, cualquier evidencia o sospecha del mal uso de los activos de información o de alguna violación a las políticas de seguridad de la COFETEL y/o a las reglas establecidas en esta guía. Esta notificación podrá hacerse de forma escrita o a título personal.
- 4.1.14 Los usuarios tienen la responsabilidad de cumplir con los procedimientos de control y requerimientos de seguridad de los accesos físicos y lógicos de los activos fijos asignados.
- 4.1.15 Es obligatorio que Los usuarios bloqueen la pantalla de su monitor cuando dejen desatendido su sistema de cómputo (ej.: cuando vayan a comer o al sanitario) ya que su equipo de computo puede ser susceptible de ser intervenido o alterado sin su consentimiento y esto origine algún tipo de problema. Es recomendable que el protector de pantalla inicie el bloqueo en un lapso de tiempo menor a los 5 minutos y que para deshabilitar esta protección sea necesario la utilización de la clave de acceso del equipo de cómputo.
- 4.1.16 Los usuarios tienen la responsabilidad de almacenar bajo llave todos los documentos y medios de almacenamiento que contengan información confidencial o de uso interno, ya sea por finalizar sus actividades diarias o por dejar desatendido su lugar de trabajo por cualquier circunstancia.

4.1.17 En caso de que los usuarios tengan asignado un equipo de cómputo portátil (laptop, PDA, entre otros) y sean víctimas de robo o pérdida del mismo, el usuario deberá reportar el incidente en un lapso no mayor a 2 horas a su área administrativa correspondiente y al Grupo de Seguridad informática.

4.1.18 Los empleados que otorguen acceso a las instalaciones de la Comisión a familiares, amigos, vecinos, clientes, proveedores, vendedores o cualquier otro tipo de visitantes deberán cumplir con los siguientes puntos:

- Verificar que se haga la identificación personal y el registro correspondiente del visitante(s) en la recepción por el personal de vigilancia.
- En caso de que el visitante(s) traiga consigo equipo de cómputo u otros objetos, verificar que éste haya sido registrado en la recepción por el personal de vigilancia.
- Verificar que el visitante(s) porte su identificación en un lugar visible en todo momento, mientras permanezca en las instalaciones de la COFETEL.
- El empleado que autorizo el ingreso del visitante(s) es el único responsable de supervisar y monitorear las acciones de la persona(s) que ingreso, y coresponsable de las acciones realizadas por el (los) visitante(s).
- El empleado tiene estrictamente prohibido el préstamo de cualquier activo o servicio de información a los visitantes. Si el visitante(s) requiriera la utilización de estos, el empleado deberá solicitar la autorización de la utilización de los activos al Grupo de Seguridad Informática el cual restringirá de acuerdo a su criterio, el acceso a los mismos. En este caso, el visitante tendrá la obligación de conocer la presente guía y por lo tanto, tendrá que firmar de conocimiento de la misma
- A la salida del visitante, verificar que se haga el registro de salida correspondiente, tanto de la persona(s) como del equipo de cómputo, si esto aplicara.
- Queda estrictamente prohibido que los proveedores autoricen acceso a cualquier persona, equipo o herramienta a las instalaciones de la COFETEL. En caso de requerir acceso de personal adicional o cualquier equipo o herramienta, el procedimiento de acceso deberá hacerse a través del empleado de la COFETEL con quien se tenga contacto

## 4.2 Uso de contraseñas

4.2.1 Los usuarios son los únicos responsables del manejo y resguardo de sus identificadores de usuario, firmas digitales y contraseñas (claves o passwords) que les den acceso a los sistemas y aplicaciones de la institución.

4.2.2 Los usuarios son los únicos responsables de todas las actividades que se realicen utilizando con sus identificadores de usuario, firmas digitales y contraseñas; incluyendo la recepción y transmisión de información, y la ejecución de

transacciones que se hagan entre los sistemas o aplicaciones de información de la COFETEL

- 4.2.3 Las contraseñas deben ser consideradas como información confidencial y privada, y por ningún motivo deberán de ser divulgadas a través de cualquier medio y/o persona alguna. Cuando, por necesidades o por requerimientos de algún proceso o sistema que afecte la integridad de la información de la COFETEL, el GSI o a la Dirección de Sistemas Informativos le solicitara al usuario esta(s), informándole las razones y repercusiones de dicha solicitud. Una vez concluida la tarea realizada, el usuario deberá cambiar la contraseña(s) para evitar cualquier problema posterior.
- 4.2.4 Los usuarios deben modificar sus contraseñas cada 30 días como máximo o con la periodicidad que el sistema o aplicación se lo requiera.
- 4.2.5 Las modificaciones de las contraseñas deben ser diferentes a las los últimos últimos 5 cambios que se hayan realizado a esta.
- 4.2.6 En caso de que un usuario intente acceder a los sistemas por más de 3 veces sin lograrlo, y su cuenta será automáticamente sea bloqueada. De inmediato deberá notificarlo a el GSI o a la Dirección de Sistemas Informativos (vía mesa de ayuda) y solicitar su reactivación, Estas instancias verificaran la autenticación del usuario y procederán en su caso, a reactivar la cuenta y generar una contraseña provisional del usuario. Este deberá cambiar la contraseña de inmediato.
- 4.2.7 El GSI o a la Dirección de Sistemas Informativos. Generan contraseñas iniciales que sólo serán válidas para el primer acceso de los usuarios. Por ello, es responsabilidad de los mismos usuarios cambiarla después de acceder al sistema por primera vez, ya que las instancias antes mencionadas no se responsabilizan de las mismas después de este acceso
- 4.2.8 Los usuarios deben utilizar una nomenclatura robusta para cumplir con la política de contraseñas de la COFETEL, considerando los siguientes elementos:
- 4.2.8.1 Se debe utilizar una combinación de al menos 8 caracteres alfanuméricos.
  - 4.2.8.2 Debe incluirse en la contraseña el uso de letras minúsculas, mayúsculas, números, caracteres especiales y espacios.
  - 4.2.8.3 No deben utilizarse solo letras, solo números, solo mayúsculas o el mismo carácter repetido.
  - 4.2.8.4 La contraseña debe ser fácil de memorizar para quien la selecciona, pero prácticamente imposible de adivinar por otra persona.
  - 4.2.8.5 No debe utilizarse el nombre o apellidos del identificador de usuario en ninguna forma (escrito al revés, doble, igual, etc.).

- 4.2.8.6 No debe utilizarse el nombre del cónyuge, hijos, familiares, novias, mascotas, fechas, etc.
- 4.2.8.7 No debe utilizarse información que pueda ser obtenida fácilmente como RFC, números telefónicos, placas de coches, direcciones, etc.
- 4.2.8.8 No deben utilizarse palabras de diccionario o genéricas (en cualquier idioma o de alguna disciplina específica como telecomunicaciones, electrónica, informática, etc.).
- 4.2.8.9 Debe utilizarse algún método para elaborar contraseñas que sea fácil de aprender y de recordar. Unos ejemplos de estos métodos son:
- Seleccionar una o varias líneas de una canción o libro y formar la contraseña con la primera letra de cada palabra.
  - Alternar entre una consonante y una o dos vocales, produciendo una palabra que sea pronunciable y de esta forma fácil de recordar.
  - Seleccionar dos palabras no relacionadas y separarlas con un caracter de puntuación.

### 4.3 Uso de Internet

- 4.3.1 El uso de Internet es un privilegio y no una obligación de la COFETEL con los usuarios.
- 4.3.2 Los usuarios no deben publicar ningún tipo de información propiedad de la COFETEL en Internet (esto incluye correo electrónico, mensajeros instantáneos, chats, blogs, redes sociales, paginas personales, etc.).
- 4.3.3 Los usuarios no deberán transmitir información confidencial (etiquetada bajo los términos del IFAI y de la misma Comisión) a través de Internet,
- 4.3.4 Los usuarios que requieran acceso a Internet, deben obtener autorización a través de su enlace administrativo, el cual hará la solicitud correspondiente al GSI quien valorará la viabilidad de dicha petición.
- 4.3.5 Las contraseñas de acceso a Internet, deben cumplir con las especificaciones de contraseñas descritas en el punto 4.2 de esta guía.
- 4.3.6 Los usuarios tienen la responsabilidad de notificar en forma inmediata al Grupo de Seguridad Informática, cualquier actividad sospechosa o evidencia de violaciones a la seguridad relacionadas con la conectividad hacia Internet (acceso no autorizado a la red, telecomunicaciones o sistemas de cómputo, transmisión aparente o real de un virus o gusano a través de la red, sabotaje aparente o real de cualquier archivo para el que el usuario haya definido un usuario y contraseña, etc.). Esta notificación podrá hacerse de forma escrita o a título personal

- 4.3.7 Los usuarios no deben utilizar los servicios de Internet para fines ilegales. En caso de no estar seguro de la legalidad de sus acciones, debe solicitar información inmediatamente al GSI.
- 4.3.8 El uso de los servicios de Internet debe limitarse a las actividades necesarias, que los usuarios requieran para el desempeño de sus funciones.
- 4.3.9 El servicio de mensajería electrónica (ej.: Microsoft Messenger, Yahoo Messenger, AOL Messenger, ICQ, Trillian, entre otros) en caso de ser un requerimiento de trabajo, deberá solicitarse autorización al titular de su área, el cual hará la solicitud correspondiente a el GSI quien valorara la viabilidad de dicha petición.
- 4.3.10 Bajo ninguna circunstancia, los usuarios pueden administrar servidores (ejm.: servidores de Web, DHCP, DNS, entre otros) en sus recursos de cómputo asignados (excepto en donde se tenga un acuerdo con el GSI).
- 4.3.11 Solamente está autorizado el tráfico de http (páginas web) y https (páginas web seguras) para acceder a Internet. Lo anterior implica que las comunicaciones a través de FTP, Telnet, Secure Shell, o páginas que lo permitan, entre otras, están prohibidas. En caso de ser un requerimiento de trabajo, deberá solicitarse autorización al Titular de su área, el cual hará la solicitud correspondiente al GSI quien valorara la viabilidad de dicha petición.
- 4.3.12 Los usuarios que no tengan acceso a Internet, tienen prohibido utilizar las cuentas de otros usuarios para obtener acceso a Internet.

*RS*

#### 4.4 **Uso de Correo electrónico**

- 4.4.1 Los usuarios tienen prohibido utilizar el correo electrónico para propósitos personales con fines distintos al desempeño de sus funciones.
- 4.4.2 Los usuarios deberán evitar acceder a cuentas de correo electrónico externas (distintas a las de la COFETEL, (@cft.gob.mx) en los recursos de cómputo asignados.
- 4.4.3 Los usuarios tienen prohibido acceder y/o usar los correos electrónicos de otros usuarios sin la autorización de estos.
- 4.4.4 Los usuarios tienen prohibido enviar o propagar mensajes tipo cadenas, archivos adjuntos de gran volumen (2 MB como máximo) o cualquier otro tipo de información que esté consumiendo innecesariamente recursos del sistema o que interfiera con el trabajo de otros usuarios.
- 4.4.5 Los usuarios tienen prohibida la falsificación o modificación de la información del encabezado de los correos electrónicos, en los que se incluye la dirección del origen, la dirección del destino y los campos de fecha y hora.



4.4.6 Los usuarios son los únicos responsables de la información transmitida con su cuenta de correo electrónico, y tienen la obligación de cumplir los siguientes lineamientos:

- El usuario deberá usar la firma autorizada.
- El mensaje de la firma no podrá ser modificado sin autorización de la Coordinación General de comunicación social,
- No deben transmitirse o recibirse secretos comerciales, información confidencial, o con derechos de autor o de propiedad.
- Esta estrictamente prohibido el manejo a través del correo electrónico de cualquier información clasificada como confidencial o de uso interno incluyendo acuerdos legales y contractuales o información técnica relacionada con las operaciones o con la seguridad de la COFETEL.
- Esta estrictamente prohibido el manejo de información de la configuración de los servidores o de la red de la COFETEL (direcciones internas de equipos, nombres de servidores, tipos de servidores, software y números de versión de software).
- No deben enviarse mensajes de correo basura (spam).
- No deben suscribirse a otros usuarios a listas de correo sin su consentimiento.
- No debe ejecutarse ningún programa, ni instalar ninguna actualización de seguridad que se reciba a través del correo electrónico o proveniente de una fuente externa. En caso de requerirlo, solicitar el apoyo al Grupo de Seguridad Informática (vía mesa de ayuda)
- Esta estrictamente prohibido utilizar el correo electrónico para transmitir o recibir mensajes que contengan material ofensivo, difamatorio o amenazante para alguna persona u organización sin su consentimiento, con o sin el fin de inflingirle algún daño emocional, profesional, económico o de cualquier otra índole.
- No debe utilizarse el correo electrónico para obtener o distribuir declaraciones, mensajes o imágenes que contengan material pornográfico, menosprecio étnico, mensajes racistas, o cualquier otro mensaje que pueda ser molesto, ofensivo o que insulte a alguna persona u organización, relacionados con religión, razas, nacionalidades, color, estado civil, ciudadanía, edad, discapacidad o apariencia física. así como juegos y cualquier otro material no relacionado con la operación de la COFETEL. La persona que reciba este tipo de material esta obligada a reportarlo al GSI.
- Cualquier declaración o comentario hecho a través del correo electrónico que en alguna forma pueda ser interpretado como una acción en nombre de la COFETEL, debe contener un mensaje de renuncia de responsabilidad como el siguiente: "Estas declaraciones reflejan solamente mi opinión y no necesariamente manifiestan la visión de la COFETEL". Adicionalmente, deben aplicarse en todas las prácticas relativas a la ética y conducta apropiadas.
- Los usuarios de correo electrónico deben conducir sus actividades teniendo en mente la reputación de la COFETEL, así mismo, deben utilizar el correo

electrónico cuidadosamente, así como cualquier otro comunicado escrito que contenga el nombre de la COFETEL.

- No deben publicarse o distribuirse las listas de correo electrónico internas a personal externo a la COFETEL.

#### 4.5 Impresión de documentos

- 4.5.1 Los equipos de impresión únicamente deben de ser utilizados para propósitos o cuestiones de trabajo de la propia institución, y relacionadas con las responsabilidades y atribuciones asignadas al usuario.
- 4.5.2 La impresión de información clasificada como confidencial o de uso interno siempre deberá incluir una etiqueta con las leyendas correspondientes a su clasificación.
- 4.5.3 Los usuarios son los únicos responsables de la custodia, manejo y almacenamiento de los documentos impresos que sean clasificados como confidenciales o de uso interno.
- 4.5.4 Cuando se imprima cualquier información, ésta debe ser removida de la impresora en forma inmediata.
- 4.5.5 Los usuarios son los únicos responsables de la destrucción de los documentos que contengan información confidencial o de uso interno que ya no sea requerida, mediante la trituración de los mismos, en los equipos destinados ex profeso para tal efecto.

#### 4.6 Entrada y salida de equipo de cómputo

- 4.6.1 Los usuarios que tengan asignado un equipo de cómputo portátil y que requieran salir de las instalaciones por cuestiones de trabajo con dicho equipo, deberán justificar el retiro y el tiempo estimado de ausencia del mismo, para así obtener una autorización escrita para la salida del equipo.
- 4.6.2 Los usuarios que tengan equipos portátiles o fijos fuera de las instalaciones de la COFETEL, tienen la responsabilidad de custodiarlos y protegerlos. Esta responsabilidad incluye toda la información que contengan dichos equipos, y esto es con el fin de mantener un grado similar de confidencialidad, privacidad y protección provista por el GSI.
- 4.6.3 Los usuarios que requieran salir o entrar a las instalaciones de la COFETEL con equipo de cómputo portátil (personal o de la institución), tienen la responsabilidad de registrarlo en la recepción con el personal de Vigilancia correspondiente.
- 4.6.4 Los usuarios que tengan equipos portátiles asignados que lo perdieran o se los roben, podrán perder permanentemente el privilegio de tener dicho equipo.

#### 4.7 Entrenamiento y concientización

- 4.7.1 Todos los usuarios sin excepción, tienen la obligación de asistir a los programas de capacitación y concientización en el tema de seguridad de la información, organizados por el GSI. En caso de no poder participar en los mismos, deberá justificarse la inasistencia obteniendo una autorización de su Jefe superior inmediato.
- 4.7.2 El desconocimiento u omisión del contenido de los programas de capacitación y concientización del tema de seguridad informática, no exime a los usuarios de las responsabilidades correspondientes en dicho tema. El desconocimiento de estos lineamientos no es excusa para su incumplimiento.

#### 4.8 Monitoreo de usuarios

- 4.8.1 El GSI se reserva el derecho de monitorear el correo electrónico, accesos a Internet, los directorios personales de archivos y otra información almacenada en los equipos propiedad de la COFETEL en cualquier momento y sin previo aviso, aún y cuando éstos contengan información personal; con el fin de asegurar el cumplimiento con las políticas de seguridad de la institución, así como con el marco legal y regulatorio a la cual la dependencia está sujeta.
- 4.8.2 Los sistemas, recursos y en general toda la información generada (incluyendo archivos, mensajes de correo electrónico y correo de voz, registros de acceso a Internet, etc.) en y para el funcionamiento de la COFETEL, son propiedad de la institución y son susceptibles de auditoría. El GSI puede interceptar y revisar, cualquier información en cualquier momento y sin previo aviso para propósitos de monitoreo, supervisión o auditoría.

#### 4.9 Virus y código malicioso

- 4.9.1 Es responsabilidad de los usuarios el utilizar el software antivirus autorizado e instalado por la DSI. Queda estrictamente prohibida la instalación de cualquier software antivirus diferente a éste.
- 4.9.2 Los usuarios tienen estrictamente prohibido modificar la configuración, eliminar, desactivar o forzar la configuración del software antivirus autorizado por el GSI.
- 4.9.3 Cualquier archivo obtenido de Internet o por algún otro medio, debe de ser revisados por el software antivirus antes de ser utilizado.
- 4.9.4 Los usuarios tienen prohibido abrir o ejecutar cualquier archivo adjunto de correo electrónico proveniente de alguna fuente desconocida, sospechosa o no confiable. Este tipo de correos debe ser borrado inmediatamente del buzón de correo electrónico y su origen debe ser declarado como no deseado.



- 4.9.5 Todos los archivos adjuntos (incluyendo el contenido de archivos comprimidos) que se reciban vía correo electrónico, aun de fuentes conocidas, deben ser revisados para detectar la presencia de algún virus y de otros programas destructivos antes de ser abiertos o almacenados en los equipos o sistemas de la COFETEL.
- 4.9.6 Los usuarios tienen la responsabilidad de revisar antes de ser utilizados, todos los medios de almacenamiento removibles (ej.: memorias USB, discos duros externos, etc.) con el software antivirus y así poder acceder sin problemas a la información contenida en ellos.
- 4.9.7 Los usuarios tienen la responsabilidad de reportar en forma inmediata al GSI (vía mesa de ayuda) cualquier incidente de virus o de código malicioso, detectados por el software antivirus instalado o por cualquier sospecha que el usuario tenga.
- 4.9.8 Los usuarios deben evitar compartir información de sus equipos con privilegios de lectura / escritura, a menos que sea absolutamente necesario para sus requerimientos de trabajo. En tal caso, se deben revisarse los equipos involucrados con el software antivirus autorizado, antes de compartir estos recursos.
- 4.9.9 Los usuarios deben borrar inmediatamente el correo electrónico no solicitado (spam o correo basura, cadenas, etc.). Queda prohibido que los usuarios reenvíen estos correos ya que son considerados peligrosos y pueden contener virus o códigos maliciosos.

#### 4.10 Herramientas de hackeo informático

- 108
- 4.10.1 El hackeo informático (adopción con fines de lucro de la reproducción, retención y/o distribución, del software o información desarrollada por otros) y cualquier otra actividades relacionadas o similares, están prohibidas. El hackeo incluye, pero no se limita, a las siguientes actividades: el acceso ilegal o no autorizado a computadoras, redes, cuentas de usuario y otros sitios restringidos; o el intento de evadir medidas de seguridad y de zonas restringidas en la red.
- 4.10.2 Los usuarios tienen prohibido descargar, instalar o ejecutar herramientas de hackeo, (programas de captura de información o sniflers, programas de acceso a usuarios externos o caballos de troya, herramientas de diagnostico de puertos y vulnerabilidades, etc.), y en general, cualquier software que pueda alterar o modificar con fines de daño o de destrucción, los sistemas y/o la información.

#### 4.11 Contenido Pornográfico.

- 4.11.1 Los usuarios tienen prohibido acceder, introducir, almacenar, desplegar, anunciar, procesar ó transmitir cualquier tipo de material pornográfico (a través de Internet o de algún otro medio), en cualquier activo de información propiedad de la COFETEL.

d



#### 4.12 RespalDOS de PC's personales

- 4.12.1 Los usuarios tienen la responsabilidad de respaldar sus archivos con información clasificada como confidencial o de uso interno. Si el usuario desconoce la forma de realizar el respaldo deberá solicitar vía mesa de ayuda la asistencia por parte del personal de Soporte Técnico.
- 4.12.2 La frecuencia con la que se debe realizar los respaldos será responsabilidad del usuario.
- 4.12.3 Los usuarios son los únicos responsables de mantener organizada su información en carpetas para facilitar y abreviar, el respaldo y la recuperación de la misma.

#### 4.13 Uso de medios removibles

- 4.13.1 Esta estrictamente prohibido el uso de medios removibles (ej.: memorias usb, discos duros, etc.) para descargar, almacenar o transmitir información de la COFETEL. En caso de requerirlo por cuestiones de trabajo, notificarlo por escrito al GSI para que esta analice el impacto de dicha petición y decidida si es procedente, y los pasos consecuentes de dicha resolución.

#### 4.14 Sanciones

- 4.14.1 Los usuarios tienen la obligación de cumplir con todas las reglas descritas en esta guía.
- 4.14.2 Los usuarios deben fomentar el cumplimiento de las políticas, estándares y procedimientos de seguridad del GSI de la COFETEL.
- 4.14.3 No existen excepciones en el cumplimiento de las reglas establecidas en esta guía. En caso de existir excepciones en su acatamiento, éstas deberán notificarse al GSI mediante un escrito de su Jefe superior inmediato en el que se justifique el requerimiento. El GSI determinará lo procedente, y los pasos consecuentes de dicha resolución.
- 4.14.4 La COFETEL se reserva el derecho de aplicar las sanciones que considere pertinentes en caso de incumplimiento por parte del usuario a las reglas establecidas en esta guía.
- 4.14.5 Las sanciones que se generen por la violación a las reglas contenidas a esta guía, son efectivas al momento en que se verifique el incumplimiento por parte del usuario.
- 4.14.6 La persona que observe cualquier incumplimiento de estos lineamientos deberá notificarlo de inmediato al GSI.

4.14.7 Las personas que incumplan con las disposiciones del presente documento se les podrá suspender el servicio de manera permanente.



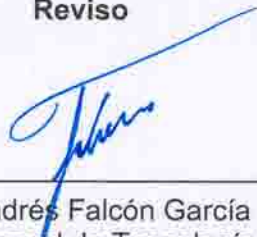
L.C.C. Guillermo Rodríguez Contreras  
Director de Sistemas Informáticos

**Elaboró**



César Vicente Pérez Gaytán  
Soporte Técnico de la Dirección de Sistemas  
Informáticos

**Reviso**



Ing. Andrés Falcón García  
Director General de Tecnologías de  
la Información y Comunicaciones

**Autorizo**



Ing. Rodrigo A. Gutiérrez Sánchez  
Coordinador General de Organización  
y Tecnologías de la Información