
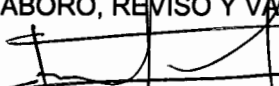
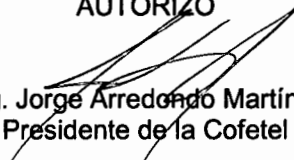



 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 1 de 25
		Fecha 10 de junio de 2005	

PROYECTO: PLAN INSTITUCIONAL DE SEGURIDAD INFORMÁTICA

**Grupo de Trabajo de Tecnologías de la Información y
Comunicaciones: Dirección de Informática, Dirección de Internet,
Dirección de Operación y Desarrollo de Sistemas, Dirección de
Soporte Técnico, Dirección de Informática y Sistemas, Dirección de
Tecnologías de la Información y Comunicaciones**

ELABORÓ 	ELABORÓ, REVISÓ Y VALIDÓ 	AUTORIZÓ 
Ing. Andrés Falcón García Director de Operación y Desarrollo de Sistemas	Ing. Juan Lozano González Director de Tecnologías de la Información y Comunicaciones	Ing. Jorge Arredondo Martínez Presidente de la Cofetel


 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 3 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

CONTENIDO


Introducción.	5
1. Alcance	6
2. Términos y definiciones	6
2.1. Estados de la información.	6
2.2. Seguridad informática	6
2.3. Evaluación de riesgos	7
2.4. Administración de riesgos	7
2.5. La DI	7
2.6. Equipo de Cómputo	7
3. Políticas de Seguridad.	7
3.1. Políticas Generales de seguridad informática.	8
4. Seguridad de la organización.	8
4.1. Infraestructura.	9
4.2. Seguridad de acceso a terceros.	9
5. Clasificación y control de activos y servicios informáticos	10
5.1. Contabilidad de activos y servicios informáticos.	10
5.2. Clasificación de la información	11
Software	11
6. Seguridad personal.	12
6.1. Seguridad en la definición de puestos y asignación de recursos.	12
6.2. Capacitación	13
6.3. Respuesta ante anomalías e incidentes de seguridad.	13
7. Seguridad física y de perímetros.	13
7.1. Perímetros seguros.	13
7.2. Seguridad de equipos.	14
7.3. Controles generales.	14
8. Administración de la operación y comunicaciones.	15
8.1. Procedimientos y responsabilidades operativas.	15
8.2. Protección contra código malicioso.	15
8.3. Mantenimiento.	16
8.4. Administración de la red.	16
8.5. Administración de los medios de almacenamiento.	16
8.6. Intercambio de información y de programas.	16

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 4 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

Correo electrónico	17
Internet	17
9. Control de acceso	18
9.1. Requerimientos del control de acceso.	18
9.2. Administración del acceso de usuarios	19
9.3. Responsabilidades de los usuarios.	19
9.4. Control de acceso remoto y de redes.	19
9.5. Control de acceso a los sistemas operativos.	20
9.6. Control de acceso a las aplicaciones.	20
9.7. Sistemas de monitoreo de acceso y uso.	20
9.8. Computo móvil y trabajo remoto	20
10. Desarrollo y mantenimiento de sistemas	21
10.1. Requerimientos de seguridad de los sistemas.	21
10.2. Seguridad en los sistemas de aplicaciones.	21
10.3. Controles criptográficos.	22
10.4. Seguridad del sistema de archivos.	22
10.5. Seguridad en el desarrollo y el proceso de soporte	22
11. Administración de la continuidad de operación	22
11.1. Aspectos de la continuidad de operación.	22
12. Cumplimiento	23
12.1. Cumplimiento de los requerimientos legales	23
12.2. Revisión de las políticas de seguridad y compatibilidad técnica.	23
12.3. Consideraciones de los sistemas de auditoría.	23
13. Bibliografía	25

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 5 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática


Introducción.

La sociedad actual es considerada como la “Sociedad de la información” y se encuentra inmersa en cuestiones tales como el manejo de grandes volúmenes de información, la globalización, la ubicuidad de las redes, el acelerado avance tecnológico de dispositivos de cómputo y comunicación, etc. En tales circunstancias, se ha considerado también a la “información” como un “activo con valor” para las organizaciones, dependencias y empresas, por lo tanto, surge la necesidad de proteger dicha información contra cualquier tipo de riesgo en que ésta pueda verse comprometida, así como también de la protección de los medios y recursos de que nos valemos para la transición entre los estados de la misma –generación, transformación, transmisión, almacenamiento y destrucción.

Actualmente la legislación, economía y sociedad mexicanas siguen la tendencia de ver en la información además de un activo, un derecho ciudadano. Si bien esto es un avance significativo, es bueno también no perder de vista que existe una amenaza latente a través del uso de canales indebidos en contra del capital que representa la información.. Dichas amenazas son de diferentes magnitudes y variedades, como pueden ser, desastres naturales, virus de computadoras, ataques de denegación de servicio, fraude asistido por computadora, espionaje, sabotaje, vandalismo y terrorismo informático entre otros.

La seguridad informática se refiere al conjunto de mecanismos destinados a minimizar los riesgos que puedan comprometer cualquiera de las características de la información, como son, la confidencialidad, integridad y disponibilidad, en cualquiera de sus estados.

En este contexto y con el fin de aprovechar todos los esfuerzos que la Comisión Federal de Telecomunicaciones (en lo subsecuente **la Comisión**) está llevando a cabo en su fase de reestructuración y reorientación como parte del proyecto SIIMAT (Sistema de Información Integral en Materia de Telecomunicaciones) y como una acción de mejora propuesta por el OIC derivado de la revisión número 05/2004, se elabora el presente Plan Institucional de Seguridad Informática con fundamento en la norma técnica ISO 17799 y que dará mayor respaldo al plan de desarrollo de actividades que tiene contempladas **la Comisión**.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 6 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

1. Alcance

El presente documento pretende ser la base inicial del Plan Institucional de Seguridad Informática de **la Comisión** que estará sujeto a un permanente proceso de mejora continua y deberá de ser observado cabalmente por sus responsables para definir, iniciar, implementar y mantener actualizado y operando el mismo. Su propósito es proveer de un fundamento técnico común para el desarrollo de estándares de seguridad en materia informática y mejores prácticas efectivas en la administración de la misma, brindando confianza en las relaciones llevadas a cabo entre las Unidades Administrativas de **la Comisión** en el uso de activos y servicios informáticos.

2. Términos y definiciones


2.1. Estados de la información.

Se refiere a cualquiera de los estados que caracterizan a la información en un lugar y tiempo determinado, estos estados pueden ser alguno de los siguientes.

- **Generación:** Es el estado que da origen a cualquier tipo de información.
- **Transformación:** Es el estado en el cual la información se encuentra en un proceso de cambio de contenido y en algunos casos de generación de nueva información.
- **Transmisión:** Es un estado en el que el contenido de la información es transferida o copiada de un medio de almacenamiento a otro.
- **Almacenamiento:** Es el estado de reposo de la información, en el cual el contenido no es alterado. Su almacenamiento puede ser temporal o permanente.
- **Destrucción:** Es el estado en que la información deja de ser importante o no será utilizada y por consiguiente se elimina dejando de existir totalmente de cualquiera de los estados anteriores.

2.2. Seguridad informática

Son el conjunto de mecanismos y buenas prácticas destinados a la preservación de las principales características de la información en cualquiera de sus estados. Dichas características son:

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 7 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

- **Confidencialidad:** Es la garantía de que todas las personas o equipos puedan acceder exclusivamente a la información que tienen autorizada.
- **Integridad:** Es la garantía y mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** Es la garantía de que las personas o equipos autorizados tienen acceso a la información y a los recursos relacionados con la misma toda vez que lo requieran.

2.3. Evaluación de riesgos

Se refiere a la evaluación de las amenazas, impactos y vulnerabilidades relativos a la información en cualquiera de sus estados y de los medios que se dispone para la transición entre estados, así como, la evaluación de la probabilidad de que ocurran.

2.4. Administración de riesgos

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.

2.5. La DI


La Dirección Informática de la Coordinación de Administración, con el Visto Bueno de la Dirección de Tecnologías de la Información y Comunicaciones de Presidencia.

2.6. Equipo de Cómputo

Entiéndase por equipo de cómputo: computadoras personales, computadoras de escritorio, PC's, Laptops, Notebooks.

3. Políticas de Seguridad.

Objetivo: Proporcionar los lineamientos en materia de seguridad informática acorde con las necesidades y recursos de **la Comisión** para mantener estándares de calidad y seguridad, evitar problemas técnicos en las PC's, evitar caer en problemas legales, eliminar la posibilidad

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 8 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones


Plan Institucional de Seguridad Informática

de contagio de virus computacionales y elevar la productividad en el uso de las herramientas de tecnologías de la información y comunicaciones.

3.1. Políticas Generales de seguridad informática.

- Es propiedad de **la Comisión**: toda la información generada dentro de **la Comisión**, la generada por terceros para **la Comisión** y la que se derive de la utilización de los recursos humanos o físicos de la misma, en cualquier lugar ajeno a **la Comisión**.
- Todo usuario de información de **la Comisión** es responsable de la utilización ética de la información de **la Comisión** que maneja dentro o fuera de su equipo de cómputo, con el único fin de cumplir con su trabajo.
- El resguardo y confidencialidad de toda la información que maneja el usuario en su equipo de cómputo, sea ésta impresa o digitalizada, es responsabilidad absoluta del funcionario, incluyendo los respaldos o copias que éste genere por motivo de sus funciones y que no deberán ser extraídos de **la Comisión**.
- La DI se reserva el derecho de entrada a las instalaciones de cómputo y comunicaciones, a las conexiones de enlaces y/o conmutadores de **la Comisión**.
- No se permite la transferencia de cualquier tipo de información a equipos de cómputo o dispositivos de almacenamiento no propiedad de **la Comisión** (es decir que sean propiedad de usuarios, proveedores, clientes, etc), salvo los que autorice expresamente el titular de la unidad administrativa correspondiente bajo su responsabilidad.
- Ningún equipo de cómputo (PC's, impresoras, scanners, modems, unidades de zip, CD's externos, quemadores externos, etcétera) puede ser reubicado sin la autorización expresa de la DI.
- Ninguna información impresa o digitalizada propiedad de **la Comisión** puede salir de las instalaciones de la misma, salvo autorización por escrito del titular de la unidad administrativa generadora de información generadora de información o bien porque así lo requiera las funciones que ejerce. La salida de esta información se realizará bajo autorización y responsabilidad del titular.
- Todos los usuarios de información de **la Comisión**, aceptan la presente política así como los procedimientos, reglamentos y sanciones que se deriven de ella, desde el momento en que son empleados (temporales o permanentes), proveedores o cualquier otro usuario que utilice información propiedad de **la Comisión**.

4. Seguridad de la organización.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 9 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

Objetivo: Definir los lineamientos de seguridad y protección física de los equipos de **la Comisión**.

4.1. Infraestructura.

- Los equipos de cómputo y comunicaciones serán utilizados exclusivamente para trabajos relacionados con las actividades de **la Comisión**.
- Queda prohibido comer, beber, fumar, almacenar alimentos o bebidas junto a los equipos.
- Ningún usuario esta autorizado a cambiar la configuración o abrir el gabinete de las computadoras, impresoras, equipo periférico o de comunicaciones. Cualquier trabajo de reparación de hardware lo tendrá que hacer el personal de la DI o el personal de proveedores externos autorizados por la DI.
- Las computadoras personales no contarán con servicios de Multimedia (bocinas), salvo autorización escrita del titular de la unidad administrativa correspondiente y el visto bueno de la DI.
- Es responsabilidad del usuario del equipo de cómputo no obstruir la salida de aire emitido por el ventilador que trae integrado la computadora a fin de evitar el sobrecalentamiento.
- Los equipos de cómputo que vayan a estar inactivos por mas de una hora deberán de apagarse tanto por seguridad como por cuestiones de ahorro de energía.
- Todo el hardware comprado o desarrollado, perteneciente a **la Comisión** o en las instalaciones de la misma es exclusivamente para fines laborales.
- Los usuarios que requieran del uso del software y hardware propiedad de **la Comisión** deberán acatar las normas establecidas y en cualquier momento son sujetas de auditoria sin previo aviso por parte de la DI. En los casos de encontrar anomalías estas serán reportadas al titular de la unidad administrativa correspondiente, DI, Recursos Humanos y Órgano Interno de Control.

4.2. Seguridad de acceso a terceros.

- Solo se permitirá la entrada a las instalaciones de cómputo y comunicaciones de **la Comisión** a todo aquel proveedor o externo que sea autorizado por la DI, , salvo aquella persona que venga a realizar alguna consulta al modulo de Transparencia de la Comisión en los equipos designados para tal efecto.
- El proveedor, durante su permanencia en las instalaciones, será acompañado por personal capacitado de **la Comisión** y designado por la DI en las actividades relacionadas con la visita.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 10 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones
Plan Institucional de Seguridad Informática

- Durante su permanencia el proveedor deberá cumplir y respetar todos los reglamentos y normas internas de **la Comisión**.
- Al proveedor no se le permitirá extraer ningún tipo de información de los equipos de **la Comisión**.
- Toda la información generada en equipos propiedad del proveedor será propiedad de **la Comisión**.
- En caso de que el proveedor tenga la necesidad de traer equipo de cómputo de su propiedad, éste deberá ser registrado en los módulos de vigilancia.
- El proveedor no podrá extraer de las instalaciones de **la Comisión** ningún equipo de hardware o software sin la autorización expresa de la DI y la Dirección de Recursos Materiales y Servicios Generales.
- En caso de manejar algún tipo de información que pertenezca a **la Comisión**, el proveedor se compromete a no divulgarla. En caso contrario se aplicarán las sanciones de ley correspondientes.

5. Clasificación y control de activos y servicios informáticos

Objetivo: Mantener un registro apropiado de los activos y servicios informáticos de **la Comisión**.

5.1. Contabilidad de activos y servicios informáticos.

- La Dirección de Recursos Materiales y Servicios Generales es la responsable del levantamiento de inventario de bienes informáticos con el apoyo técnico de la DI.
- Todos los usuarios deberán firmar un resguardo del equipo informático asignado para sus labores.
- Queda prohibido que cualquier usuario cambie un equipo informático o aparato telefónico por otro o mueva equipo informático o telefónico de lugar.
- El personal de la DI es el único autorizado para realizar movimientos de equipo.
- En caso de que algún usuario requiera de la instalación de software, hardware, correo, Internet o acceso a sistemas propiedad de **la Comisión**, la DI asignará a una persona responsable para la instalación.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 11 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones
Plan Institucional de Seguridad Informática

5.2. Clasificación de la información

Software

- Todo el software de **la Comisión** deberá ser instalado por personal de la DI, es decir que ningún usuario puede instalar software de manera directa.
- El software autorizado para uso en las computadoras de **la Comisión** es el siguiente:
 - Microsoft Windows 95 / 98 / Windows 2000 / Windows XP o cualquier otra versión de Windows que sea liberada por Microsoft.
 - Microsoft Internet Explorer, Word, Excel, Power Point, Visio y Project
 - Emulador de Terminales Hotware.
 - Adobe Acrobat Reader y Acrobat Reader Pro, After Effects, Page Maker, Photoshop e Illustrator.
 - Corel Draw
 - Mind Manager x5 Pro
 - El único antivirus autorizado en **la Comisión** es Norton Antivirus
 - Macromedia Director MX y Studio MX
 - Cliente de Progress
 - Cliente de Oracle
 - Microsoft Outlook para utilizar el correo electrónico interno y para utilizar cuentas de correo de Internet (Exclusivamente la cuenta @cft.gob.mx). Ningún usuario podrá recibir o enviar correos de Internet en otro tipo de cuenta).

Nota: La lista antes mencionada se puede modificar, ampliar o acortar en cualquier momento lo cual se hará del conocimiento de los usuarios de la Comisión.

- Cualquier software no incluido en la lista anterior que sea requerido por los usuarios, incluido shareware o freeware, deberá ser solicitado por escrito por la Dirección General del área requirente y será evaluado por la DI y puesto a consideración del Comité de Informática.
- Queda prohibido el utilizar los equipos de cómputo para juegos electrónicos (incluidos o no dentro del software preinstalado)

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 12 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

- Queda prohibido la instalación y utilización de paquetes comerciales de cómputo que no cuenten con la licencia de uso respectiva y de paquetes de demostración que entreguen proveedores o externos o que se bajen por Internet.
- En caso de utilizar cualquier paquete sin licencia e incurrir en violaciones a la Ley Federal de Derechos de Autor, el usuario será responsable directamente.
- Sin excepción, ningún software NO autorizado (no incluido en la lista anterior) podrá estar instalado en los equipos de computo de Cofotel, .
- No se permite bajar de Internet ningún tipo de archivo que no este directamente relacionado con las funciones de **la Comisión**, como por ejemplo cualquier archivo de música (MP3,RA, WAV, etc.), archivos de video que no sean documentos de capacitación autorizados por Dirección de Recursos Humanos y la DI.
- Todo el software comprado o desarrollado, perteneciente a **la Comisión** o en las instalaciones del mismo será utilizado exclusivamente para fines laborales.
- La DI se reserva el derecho de auditar los equipos informáticos en cualquier momento y sin previo aviso para asegurar el adecuado cumplimiento de estas políticas.

6. Seguridad personal.

Objetivo: Identificar las responsabilidades sobre los activos y servicios informáticos asignados.

6.1. Seguridad en la definición de puestos y asignación de recursos.

- Todo el personal (interno y externo) que labore en **la Comisión** se obliga a cumplir con cada una de las normas, políticas, manuales y procedimientos de seguridad instaurados por **la Comisión**.
- Todo el personal relacionado con el Grupo de Trabajo de Tecnologías de la Información y Comunicaciones deberá portar su credencial, en un lugar visible, que lo acredite como funcionario de **la Comisión**.
- Todo el personal externo que labore en **la Comisión** para asuntos relacionados con tecnologías de la información y comunicaciones deberá portar su credencial de externo, en un lugar visible, que lo acredite como visitante.
- Todo el personal interno y externo que labore en **la Comisión** se compromete a mantener de manera confidencial toda la información que pudiera conocer derivado de las actividades encomendadas.
- No se le permite a ninguna persona sacar equipo de cómputo de las instalaciones salvo autorización expresa de la DI y de la Dirección de Recursos Materiales y Servicios

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 13 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

Generales y para tales casos se tendrá que informar por escrito el motivo de la salida del equipo.

- Todo el personal tanto interno como externo es responsable del buen uso de la información que tiene a su cargo.
- Cualquier persona que viole los derechos de confidencialidad de la información propiedad de **la Comisión** se hará acreedora a la sanción legal correspondiente.

6.2. Capacitación

- Las presentes políticas son para el conocimiento y cumplimiento de todo el personal que labore en **la Comisión**, así como de terceros que por alguna razón utilicen los equipos de **la Comisión**.
- El Plan Institucional de Seguridad Informática será difundido a toda **la Comisión** vía la Intranet. La DI apoyará a cualquier usuario en su entendimiento y observancia.
- Cualquier persona que labore en **la Comisión** acepta las presentes políticas.

6.3. Respuesta ante anomalías e incidentes de seguridad.


- Cualquier anomalía respecto al no cumplimiento de las presentes políticas será reportada al titular de la unidad administrativa correspondiente, al Órgano Interno de Control, al Director de Recursos Humanos y a la DI para determinar la gravedad de la falta y tomar las acciones necesarias.

7. Seguridad física y de perímetros.

Objetivo: Definir los perímetros de seguridad y prevenir el acceso no autorizado, daños o interferencia en los sitios destinados a resguardar los activos informáticos.

7.1. Perímetros seguros.

- Salvo autorización expresa de la DI, no se le permite la entrada a ninguna persona a los centros de cómputo y comunicaciones de **la Comisión**.
- Los equipos de cómputo que no estén en uso serán retirados y resguardados por personal de la DI en el entendido, de que si algún equipo no se encuentra bajo resguardo de algún funcionario, la DI podrá o bien asignarlo a otro funcionario que lo requiera con

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 14 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

base en las necesidades detectadas o retirarlo para su resguardo en los lugares asignados para tal efecto.

7.2. Seguridad de equipos.

- Queda prohibido comer, beber, fumar, almacenar alimentos o bebidas junto a los equipos.
- Ningún usuario esta autorizado a cambiar la configuración o abrir el gabinete de las computadoras, impresoras, equipo periférico o de comunicaciones. Cualquier trabajo de reparación de hardware lo tendrá que hacer el personal de la Dirección de Informática.
- Sin excepción alguna, todos los usuarios de equipo de cómputo de **la Comisión** tienen la responsabilidad de no jalar, romper, torcer o dañar ninguno de los cables conectados al equipo. Cualquier anomalía podrá ser reportada a la DI.
- Queda prohibido conectar cafeteras, ventiladores, sacapuntas, hornillas, aspiradoras y cualquier aparato electromecánico a los enchufes de color naranja y a los enchufes de las mamparas.
- Es responsabilidad del usuario de equipo de cómputo no obstruir la salida de aire emitido por el ventilador que trae integrado la computadora a fin de evitar el sobrecalentamiento.
- Ningún usuario está autorizado para mover los equipos de cómputo de **la Comisión**. Estos movimientos los realizará exclusivamente el personal autorizado por la DI.
- Los equipos que se identifiquen para baja serán entregados por la DI a la Dirección de Recursos Materiales y Servicios Generales para que realice el trámite administrativo correspondiente.
- Ningún usuario tendrá acceso a las funciones siguientes:
 - Panel de control.
 - Ejecutar archivos directamente.
 - Creación de directorios compartidos en PC. Si se requiere compartir información deberá hacerse vía servidores solicitando este servicio a la DI
 - Instalación del Software (solo puede hacerlo personal de la DI).
 - Explorar la Red
 - Ventana de DOS
 - RegEdit

7.3. Controles generales.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 15 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

- Por seguridad de los equipos y los usuarios, no se permite pegar ningún tipo de estampa (postit, propagandas, caricaturas, etcétera) en los equipos de cómputo de **la Comisión**.
- Por seguridad de los equipos y los usuarios, no se permite colocar ningún objeto (muñecos, calendarios, papeles, bolsas, vasos, etcétera) arriba de los monitores propiedad de **la Comisión** por el riesgo de sobrecalentamiento de los equipos.

8. Administración de la operación y comunicaciones.


Objetivo: Asegurar la correcta operación de las instalaciones de procesamiento, minimizar riesgos o fallas de los sistemas, preservar la integridad y disponibilidad de los activos informáticos, así como, prevenir el mal uso de los mismos.

8.1. Procedimientos y responsabilidades operativas.

- Los funcionarios definidos por la DI serán los responsables de llevar a cabo los procedimientos de administración previamente establecidos.
- Los funcionarios definidos por la DI serán los responsables del buen funcionamiento del hardware y sistema operativo de los servidores y de comunicaciones.
- Los responsables definidos por la DI serán los responsables de la recuperación de los servidores y equipos de comunicaciones en caso de una contingencia, siendo responsabilidad del área de desarrollo poner en funcionamiento la aplicación.
- La DI deberá tener una carpeta de procedimientos de cada uno de los servidores y equipos de comunicaciones que ésta administre sobre su operación, administración, respaldos, recuperación, etc.

8.2. Protección contra código malicioso.

- A fin de proteger los equipos de cómputo de **la Comisión**, todos deberán tener instalado el software antivirus autorizado por la DI.
- A fin de evitar la entrada de virus, no se permite la instalación de ningún software que no sea propiedad de **la Comisión**.
- Los usuarios no deberán desinstalar el software antivirus.
- Cualquier problema de virus deberá ser reportado al personal de la DI de inmediato para su solución.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 16 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

8.3. Mantenimiento.

- La DI será responsable de administrar los contratos de Mantenimiento de equipos de hardware y herramientas de software con que cuenta **la Comisión**.
- Se anexa a este Plan Institucional de Seguridad Informática la carpeta de contratos de mantenimiento de la Dirección de Informática.


8.4. Administración de la red.

- No se permite la entrada a ninguna persona a las instalaciones donde se almacena el equipo de comunicaciones y servidores.
- No se permite que ninguna persona no autorizada por la DI configure, administre los servidores y equipos de comunicaciones de **la Comisión**.
- Todos los servidores y equipos de comunicaciones deberán tener un usuario y clave especiales para entrar y solo el personal de la DI, o el autorizado por ésta, lo podrá conocer para realizar actividades propias de la administración.

8.5. Administración de los medios de almacenamiento.

- Los respaldo se realizan en cintas DDS 1, 2 , 3 y 4.
- Estas cintas están disponibles en el Almacén General de **la Comisión** y son para uso exclusivo de las áreas de informática de **la Comisión**.
- Las cintas son exclusivas para los respaldos de información de los servidores y aplicaciones de **la Comisión**.
- Las cintas podrán ser utilizadas tantas veces sea necesario siempre y cuando no estén dañadas o no excedan la vida útil definida por el fabricante de las mismas.
- Ningún usuario deberá tener unidades de CD-RW a su servicio, salvo solicitud expresa del titular de la unidad administrativa correspondiente y visto bueno de la DI.
- La DI se reserva el uso de unidades de CD-RW para la realización de respaldos de programas, sistemas, bases de datos, etcétera.
- La DI contará con un manual y registro de las fechas de Respaldos y se realizaran bitácoras de cada uno de los respaldos realizados.

8.6. Intercambio de información y de programas.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 17 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

Correo electrónico

- El usuario dueño del buzón es responsable de todo tipo de mensajes y archivos que sean emitidos desde el mismo.
- La contraseña (password) del buzón personal deberá ser cambiada al menos cada 30 días, siendo esta responsabilidad directa del usuario
- Los buzones del correo electrónico son personales e intransferibles.
- El usuario podrá solicitar apoyo a la DI para programar una clave de acceso al archivo de mensajes y de esta manera asegurar que nadie pueda leer los mensajes previamente recibidos y/o enviados.
- El uso seguro del correo electrónico indica que por ningún motivo se deje abierto el software de correo electrónico o bandeja de entrada sin atención del usuario a su equipo.
- El uso del correo electrónico esta restringido para el envío de mensajes de interés para las actividades propias del puesto que desempeña el usuario. Es decir, se prohíbe el envío de: fotografías, imágenes y dibujos (excepto aquellas requeridas para el trabajo mismo del usuario), archivos ejecutables, textos de compra/venta de artículos, felicitaciones personales, insultos, cadenas, juegos, etc.
- Para reducir la saturación del correo, se recomienda evitar enviar correos con respuestas obvias, tales como O.K., enterado y otras.
- Ningún usuario deberá enviar correos masivos (a todos los usuarios) . Estos deberán ser enviados desde la cuenta del Administrador del Sistema. Para tal efecto deberán comunicarse a la DI. Lo anterior se podrá exceptuar cuando exista una causa justificada (emergencia) que así lo amerite.
- Se recomienda que el usuario revise su correo por lo menos tres veces al día para evitar la saturación de su cuenta.
- Se recomienda que todos los correos que no se utilicen deberán ser eliminados permanentemente para evitar la saturación del Microsoft Outlook.

Internet

- Los recursos informáticos no son ilimitados. El ancho de banda de la red y la capacidad de almacenamiento tienen límites finitos, y todos los usuarios conectados a la red tienen la responsabilidad de conservar estos recursos. Por tal motivo, el usuario no debe realizar deliberadamente actos que representen un mal uso de los recursos informáticos ni monopolicen los recursos injustamente en detrimento de los demás. Estos actos incluyen, entre otros: enviar correo masivo o cartas de cadena, pasar períodos prolongados navegando en Internet, jugar, participar en charlas en línea, cargar o descargar archivos de gran tamaño que no estén comprimidos (un archivo mayor a

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 18 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

10Mb se considera de gran tamaño), acceder a archivos de audio o vídeo de emisión continua (streaming audio o video) o crear de cualquier otra forma cargas innecesarias en el tráfico de la red asociadas con el uso de Internet que no se relacione con las actividades de **la Comisión**.


- Los usuarios son responsables del uso ético, legal y profesional sobre la consulta y acceso a Internet.
- Todos los usuarios de Internet se comprometen a utilizarlo exclusivamente para funciones concernientes a **la Comisión** y en caso de recibir información ajena a la misma eliminarla inmediatamente.
- Todos los usuarios de Internet serán sujetos de auditoría sin previo aviso.
- Queda prohibido el acceso a sitios de Internet que contengan material sexualmente explícito o cualquier otro material que se considere inapropiado u ofensivo en el lugar de trabajo.
- La DI se reserva el derecho de utilizar software o hardware que permita la identificación en línea y bloqueo del acceso a sitios específicos de Internet.
- No se permite bajar archivos de música, emisión continua (radio, por ejemplo), correo basura (cadenas, chistes, etcétera), barras de navegación, juegos y cualquier otro tipo de información que no esté relacionada con **la Comisión** o con las funciones propias de la plaza a la que se esta a cargo.
- No se permite el abuso en la utilización de herramientas de mensajería emergente (Messenger y similares) salvo para fines estrictamente laborales y de comunicación con personal interno de **la Comisión**.

9. Control de acceso

Objetivo: Prevenir el acceso y diseminación no autorizada a los activos y servicios informáticos mediante el uso de mecanismos de registro, autenticación y validación de identidades y roles.

9.1. Requerimientos del control de acceso.

- No se permite el acceso a los servidores y equipos de comunicaciones por ninguna persona no autorizada por la DI.
- En las computadoras personales no esta permitido que ningún usuario se firme como "administrador del sistema", ésta característica esta reservada exclusivamente para tareas de administración de los equipos para el personal autorizado de la DI.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 19 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

9.2. Administración del acceso de usuarios

- Los privilegios para el uso de recursos informáticos específicos (contraseñas de acceso) deberán ser solicitados por el titular de la unidad administrativa correspondiente con el visto bueno de la DI.
- En caso de que algún usuario cause baja de **la Comisión**, todos los accesos anteriormente definidos serán clausurados por lo que la Dirección de Recursos Humanos informará de estas eventualidades a la DI.
- Será responsabilidad de los usuarios tanto el buen manejo de los recursos y contraseñas para acceso a sistemas específicos como la confidencialidad de la información que se maneja. Cualquier abuso o uso ineficiente de la información manejada será reportada al titular de la unidad administrativa correspondiente, a la DI, a la Dirección de Recursos Humanos y al Organismo Interno de Control de **la Comisión** para establecer la sanción correspondiente.

9.3. Responsabilidades de los usuarios.

- Será responsabilidad del usuario el buen uso de la/las contraseñas entregadas para el acceso a los recursos informáticos.
- El usuario no deberá entregar su contraseña a ninguna otra persona.
- Es responsabilidad del usuario la confidencialidad de la contraseña asignada.
- El usuario deberá cambiar su contraseña por lo menos una vez al mes y podrá solicitar ayuda a la DI para el cambio de la misma.
- El usuario no deberá anotar la contraseña en ningún papel.
- Las contraseñas no deberán tener palabras como su nombre, fecha de nacimiento, nombres de los hijos, marcas y en general ninguna palabra que sea sencilla de adivinar.
- Las contraseñas deberán tener por lo menos dos caracteres numéricos y una letra mayúscula.
- No se recomienda utilizar la misma contraseña para todos los sistemas que utilice el usuario.
- El resguardo firmado por los usuarios los compromete a cuidar el equipo y hacer buen uso de el mismo y de la información en el contenido.

9.4. Control de acceso remoto y de redes.

- El acceso remoto a sistemas y equipos de **la Comisión** está restringido y solo será concedido a usuarios internos previa solicitud por escrito del titular de la unidad

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 20 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones
Plan Institucional de Seguridad Informática

administrativa correspondiente o a usuarios externos (proveedores) previa autorización de la DI.

9.5. Control de acceso a los sistemas operativos.

- En las computadoras personales y portátiles no está permitido que ningún usuario se firme como “administrador del sistema”, ésta característica está reservada exclusivamente para tareas de administración de los equipos para el personal autorizado de la DI.
- Únicamente el personal autorizado por la DI tendrá acceso como “administrador del sistema” en los servidores y equipos de comunicaciones.
- Estas contraseñas no serán de uso público y podrán ser cambiadas cada vez que se considere necesario o por lo menos una vez al mes.

9.6. Control de acceso a las aplicaciones.

- Las aplicaciones desarrolladas por **la Comisión** deberán tener, por lo menos, una contraseña al inicio para permitir la entrada de los usuarios a éstas.
- Únicamente las aplicaciones que sean para libre consulta, como la intranet, no tendrán contraseñas.

9.7. Sistemas de monitoreo de acceso y uso.

- Por el momento no se tienen sistemas de monitoreo de acceso y uso, sin embargo, el personal de la DI podrá gestionar en cualquier momento la compra de este tipo de software para realizar acciones de monitoreo sobre los recursos informáticos.
- Así mismo la DI se reserva el derecho de realizar inspecciones a los equipos de cómputo para verificar el cumplimiento de este Plan Institucional de Seguridad Informática y en el caso de encontrar anomalías estas serán reportadas al Órgano Interno de Control.

9.8. Computo móvil y trabajo remoto

- Las computadoras portátiles (notebooks) deberán seguir las mismas políticas que las de las computadoras personales.
- Los usuarios que tengan computadoras portátiles serán responsables del buen manejo de los equipos.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 21 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

- Por ser un equipo de **la Comisión**, toda la información generada y almacenada en las computadoras portátiles pertenece a **la Cofetel**.
- Cualquier usuario que desee retirar el equipo portátil asignado para trabajo fuera de la oficina deberá obtener autorización expresa de la DI y la Dirección de Recursos Materiales y Servicios Generales.

10. Desarrollo y mantenimiento de sistemas


Objetivo: Prever la debida integración de las políticas de seguridad existentes en el desarrollo, adquisición o mantenimiento de los sistemas, previniendo la pérdida, modificación o uso no autorizado de la información.

10.1. Requerimientos de seguridad de los sistemas.

- Se tendrá un servidor especialmente dedicado para el desarrollo de los sistemas.
- No se realizará ningún desarrollo sobre los servidores en producción.
- Una vez que el servidor entre en producción, se deberá contar con uno de pruebas/manteniendo, donde se llevarán a cabo las adecuaciones y pruebas necesarias antes de pasarlas a producción.

10.2. Seguridad en los sistemas de aplicaciones.

- Las aplicaciones deberán residir en los servidores de **la Comisión** o en los equipos que se determine que cuentan con las características técnicas suficientes para soportar la aplicación.
- Únicamente el personal autorizado por la DI tendrá acceso a la administración del sistema operativo del equipo donde reside el sistema.
- Será responsabilidad de la DI el hardware y sistema operativo del servidor donde reside la aplicación.
- Todas las aplicaciones que soporten accesos de usuarios vía Internet serán instaladas fuera de la Comisión en las instalaciones del ISP (Internet Service Provider) que sea contratado para tal efecto.
- Será responsabilidad del área encargada del desarrollo, la aplicación misma y su correspondiente base de datos.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 22 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones
Plan Institucional de Seguridad Informática

10.3. Controles criptográficos.

- Por el momento no se requieren de controles criptográficos para el desarrollo de las aplicaciones de **la Comisión**.

10.4. Seguridad del sistema de archivos.

- Durante el desarrollo y mantenimiento a los sistemas la DI hará un respaldo de la información con una periodicidad diaria incremental y semanal total o cada vez que se considere necesario.
- Ningún usuario no autorizado por la DI tendrá acceso a los archivos fuente del desarrollo en cuestión.

10.5. Seguridad en el desarrollo y el proceso de soporte


- Se definirá un directorio explícito durante para el desarrollo y mantenimiento de los sistemas y no afectar el ambiente de producción.
- El desarrollo de sistemas no se deberá realizar en el servidor de producción.
- Todo el código desarrollado por personal externo a **la Comisión** y que se utilice para las actividades de ésta, pertenecerá a la Cofetel y cualquier violación a la confidencialidad de la información por parte del proveedor o desarrollador se hará acreedor a las sanciones propias que la ley determine.

11. Administración de la continuidad de operación

Objetivo: Minimizar los tiempos de interrupción de operación y uso de los activos y servicios informáticos por acciones deliberadas o accidentales. Esto es para mejorar el aprovechamiento de los sistemas e información que operan las diferentes Unidades Administrativas que integran **la Comisión** para el desarrollo y cumplimiento de sus actividades.

11.1. Aspectos de la continuidad de operación.

- La DI definirá y evaluará los procedimientos para asegurar la continuidad de la operación de los sistemas de **la Comisión** y de las comunicaciones que ésta requiere.
- En un esquema de contingencia se entiende que no todos los usuarios podrán tener acceso a todas las aplicaciones que normalmente tienen en sus computadoras, por lo

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 23 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

que solo aquellos usuarios definidos como prioritarios para cada sistema podrán continuar trabajando en el entendido que la velocidad de respuesta será menor.

- La DI llevará una bitácora diaria de eventos en la que anotará, cuando existan fallas en cualquier sistema, equipo de cómputo o telecomunicaciones, datos precisos sobre fecha y hora de ocurrencia del evento, fecha y hora en que se detectó, reporte levantado (si existe), usuario o usuarios afectados, proveedor involucrado y contrato de mantenimiento si aplica, fecha y hora en que se corrigió, tiempo en el que la operación estuvo interrumpida, persona o personas que lo corrigieron, razón de la falla, proceso de solución, esquema de contingencia utilizado y mecanismos implementados para asegurar que la falla no vuelva a ocurrir.

12. Cumplimiento

Objetivo: Prevenir y evitar violaciones a las leyes, normas, reglamentos, contratos y requerimientos de seguridad contractuales.

12.1. Cumplimiento de los requerimientos legales

- Es responsabilidad de los usuarios apearse a la legislación vigente.
- Es responsabilidad de los usuarios apearse a los manuales de organización y procedimientos de las distintas Unidades Administrativas.
- Es responsabilidad de los usuarios apearse la ley de derechos de copiado y de propiedad intelectual.
- Es responsabilidad de los usuarios apearse a este Plan Institucional de Seguridad Informática.

12.2. Revisión de las políticas de seguridad y compatibilidad técnica.

- Las presentes políticas se deberán revisar y actualizar por lo menos cada 3 meses o cada vez que la Dirección de Tecnologías de Información y Comunicaciones lo considere necesario en un esfuerzo constante de mejora continua.

12.3. Consideraciones de los sistemas de auditoría.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 24 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

- La DI será la única que podrá autorizar el software o herramientas necesarias para una auditoría informática
- La Dirección de Tecnologías de Información y Comunicaciones podrá autorizar y definir los alcances, acuerdos y controles de auditoría necesarios para el cumplimiento de las presentes políticas.

 Comisión Federal de Telecomunicaciones	COMISIÓN FEDERAL DE TELECOMUNICACIONES	Codificación CFT-PISI-02	
		Revisión 2	Página 25 de 25
		Fecha 10 de junio de 2005	

Área responsable: Grupo de Trabajo de Tecnologías de la Información y Telecomunicaciones

Plan Institucional de Seguridad Informática

13. Bibliografía

- ISO/IEC 17799:2000 - Information technology. Code of practice for information security management.
- Apuntes del “Diplomado de Seguridad Informática”, 7ª Generación, CEM Polanco-UNAM.