"MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS"

Elaboró	Aprobó	Autorizó
Pedro Arriola Padilla Jefe del Departamento de Desarrollo de Sistemas	Subdirector Administrativo	**Froylán Hernández Ruiz** Director Administrativo y Financiero

Historia del Documento

Control de Cambios

Fecha de elaboración	Fecha autorización	Versión	Elaboró	Naturaleza del cambio
04/01/2010		1.0	Pedro Arriola Padilla	Creación

Revisado por

Área / Dirección	Persona
Departamento de Desarrollo de Sistemas	Pedro Arriola Padilla

Copia para

Área / Dirección	Persona
Áreas del FIFONAFE	Todo el personal del FIFONAFE

C O N T E N I D O

Manual de Políticas y Estándares de Seguridad Informática

Propósito

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del Fideicomiso Fondo Nacional de Fomento Ejidal (FIFONAFE).

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las políticas y estándares.

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades del FIFONAFE en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal.
- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Cumplimiento.

Estas políticas en seguridad informática se encuentran alineadas con el Estándar Británico BS7799.

Marco – Jurídico Administrativo

La **"Ley Federal de Responsabilidades Administrativas de los Servidores Públicos",** en el Artículo 8, Fracción III y V, se señalan las siguientes obligaciones: "Utilizar los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, exclusivamente para los fines a que están afectos;" y "Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad e impedir o evitar su uso, sustracción, destrucción, ocultamiento o inutilización indebidos"

La **"Ley Federal de Derechos de Autor",** que tipifica como delito el

que reproduzca, distribuya, venda o arriende un programa de computación sin autorización del titular de los derechos de autor; así como lo que establece el texto del artículo 103 “Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste” así como lo establecido en el Artículo 105 “El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando: I. Sea indispensable para la utilización del programa, o II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación”.

Y en caso de incumplir las presentes disposiciones, el responsable o responsables se podrán hacer acreedores a una sanción, de acuerdo a lo establecido en el Artículo 231 “Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:…”VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular” y en el Artículo 232 del Título XII, Capítulo II. De las Infracciones en materia de comercio de la mencionada Ley, y en materia de comercio previstas en la presente Ley, serán sancionadas por el Instituto Mexicano de la Propiedad Industrial como multa:

De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, V, VII (Usar, reproducir o explotar una reserva de derechos protegidos o un programa de cómputo sin el consentimiento del titular); VIII y IX del Artículo anterior.

La **“Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental”**, Artículo 63, Frac. I, que señala la responsabilidad administrativa de los servidores públicos por “Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión”

Objetivo	Difundir las políticas y estándares de seguridad informática a todo el personal del FIFONAFE, para que sea de su conocimiento y cumplimiento en los recursos informáticos utilizados o asignados.
Alcance	El documento describe las políticas y los estándares de seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del FIFONAFE.
Justificación	El Departamento de Desarrollo de Sistemas está facultado, para definir políticas y estándares en materia de informática.
Sanciones por incumplimiento	El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.
Beneficios	Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información del FIFONAFE.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política

Todo usuario de bienes y servicios informáticos deben de firmar un convenio en el que acepte las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del FIFONAFE, así como el estricto apego al *Manual de Políticas y Estándares de Seguridad Informática para Usuarios*.

Los usuarios deberán cumplir con lo establecido en el Manual de *Políticas y Estándares de Seguridad Informática para Usuarios*.

1.1 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las *Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.*

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos del FIFONAFE deben firmar de aceptación el convenio de confidencialidad y uso adecuado de los recursos informáticos y de información del FIFONAFE, así como comprometerse a cumplir con lo establecido en el Manual de *Políticas y Estándares de Seguridad Informática para Usuarios.*

1.3 Entrenamiento en seguridad informática

Todo empleado del FIFONAFE de nuevo ingreso deberá de contar con la inducción sobre el *Manual de Políticas y Estándares de Seguridad Informática para Usuarios,* a través de la Subdirección Administrativa donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

1.4 Medidas disciplinarias

1.4.1. Cuando la Subdirección Administrativa identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Órgano Interno de Control del FIFONAFE, para los efectos de su competencia y atribuciones.

1.4.2. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial del FIFONAFE, o de que se le declare culpable de un delito informático.

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del FIFONAFE sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y el centro de cómputo del FIFONAFE.

2.1 Resguardo y protección de la información

2.1.1. El usuario deberá reportar de forma inmediata a la Subdirección Administrativa, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2. El usuario tiene la obligación de proteger los discos, disquetes, cintas magnéticas y CD-ROM que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

2.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información del FIFONAFE que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2 Controles de acceso físico

2.2.1. Cualquier persona que tenga acceso a las instalaciones del FIFONAFE, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del FIFONAFE, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

2.2.2. Las computadoras personales, las computadoras portátiles, módems, y cualquier activo de tecnología de información, podrá salir de las instalaciones del FIFONAFE únicamente con la autorización de salida de la Oficina de Bienes Muebles.

2.3 Seguridad en áreas de trabajo

El centro de cómputo del FIFONAFE es área restringida, por lo que sólo el personal autorizado por el Departamento de Desarrollo de Sistemas puede acceder a él.

2.4 Protección y ubicación de los equipos

2.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Departamento de Sistemas, en caso de requerir este servicio deberá solicitarlo al Centro de Atención a Usuarios (Departamento de Desarrollo de Sistemas).

2.4.2. El área de control de bienes muebles será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Departamento de Desarrollo de Sistemas.

2.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del FIFONAFE.

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

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro identificada como “datos” o similares, ya que las otras están destinadas para archivos de programa y sistema operativo.

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

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

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad

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

2.4.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al Centro de Atención a Usuarios a través de un plan detallado de movimientos debidamente autorizados por el director del área que corresponda.

2.4.11. Queda prohibido que el usuario abra o desarme los equipos de cómputo.

2.5 Mantenimiento de equipo

2.5.1. Únicamente el personal autorizado por el Departamento de Desarrollo de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2. Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

2.6 Pérdida de Equipo

2.6.1. El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.6.2. El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3. El usuario deberá dar aviso inmediato al área de sistemas, Órgano Interno de Control y Oficina de Control de Bienes Muebles de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7 Uso de dispositivos especiales

2.7.1. El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.7.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del director correspondiente.

2.7.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.7.4. Queda prohibido el uso de módems externos en las computadoras de escritorio.

2.7.5. Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por su Subdirector.

2.7.6. Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la

Comisión para conectarse a ningún servicio de información externo.

2.8 Daño del equipo

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso el Departamento de Desarrollo de Sistemas determinará la causa de dicha descompostura,

3. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica del FIFONAFE. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del FIFONAFE o hacia redes externas como Internet.

Los usuarios del FIFONAFE que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

3.1 Uso de medios de almacenamiento

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido (File Share), deberá contar con la autorización del área dueña de la información. El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá de presentarla al Departamento de Desarrollo de Sistemas firmada por su Director de área de adscripción.

3.1.2. Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo.

3.1.3. En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito al Departamento de Desarrollo de Sistemas y con la firma del Director del área correspondiente.

3.1.4. Los usuarios de informática del FIFONAFE deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Comité de Información del FIFONAFE, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

3.1.5. Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información del FIFONAFE son registradas y susceptibles de auditoria.

3.2 Instalación de software.

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad del FIFONAFE, deberán justificar su uso y solicitar su autorización al Departamento de Desarrollo de Sistemas, a través de un oficio firmado por su Dirección de adscripción, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

3.2.2. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del FIFONAFE, que no este autorizado por el Departamento de Desarrollo de Sistemas.

3.3 Identificación del incidente

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Centro de Atención a Usuarios (CAU) lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar a su Director de adscripción.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del FIFONAFE debe ser reportado al Centro de Atención a Usuarios (CAU).

3.4 Administración de la configuración

Los usuarios de las áreas del FIFONAFE no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del FIFONAFE, sin la autorización del Departamento de Desarrollo de Sistemas.

3.5 Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Departamento de Desarrollo de Sistemas, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del FIFONAFE, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

3.6 Uso del Correo electrónico

3.6.1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al FIFONAFE, a menos que cuente con la autorización de la Dirección de adscripción.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del FIFONAFE. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuándo vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones

3.6.4. El FIFONAFE se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática del FIFONAFE o realizado acciones no autorizadas.

3.6.5. El usuario debe de utilizar el correo electrónico del FIFONAFE única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.

3.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito al área de Atención a Usuarios, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director del área que corresponda.

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

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

3.7 Controles contra código malicioso

3.7.1. Para prevenir infecciones por virus informático, los usuarios del FIFONAFE no deben hacer uso de cualquier clase de software que no

haya sido proporcionado y validado por el Departamento de Desarrollo de Sistemas.

3.7.2. Los usuarios del FIFONAFE deben verificar que la información y los medios de almacenamiento, considerando al menos discos flexibles, CD's, cintas y cartuchos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Departamento de Desarrollo de Sistemas.

3.7.3. Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

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

3.7.5. Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Departamento de Desarrollo de Sistemas.

3.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Centro de Atención a Usuarios (CAU) para la detección y erradicación del virus.

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar al Centro de Atención a Usuarios periódicamente las actualizaciones del software antivirus.

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

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario del FIFONAFE debe intentar erradicarlos de las

computadoras.

3.8 Internet

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

3.8.2. La asignación del servicio de Internet, deberá solicitarse por escrito al Centro de Atención a Usuarios, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del subdirector del área correspondiente.

3.8.3. Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el FIFONAFE.

3.8.4. Los usuarios de Internet del FIFONAFE tienen que reportar todos los incidentes de seguridad informática al Departamento de Desarrollo de Sistemas a través del Centro de Atención a Usuarios (CAU) inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.5. El acceso y uso de módem en el FIFONAFE tiene que ser previamente autorizado por el Departamento de Desarrollo de Sistemas.

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

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del Departamento de Desarrollo de Sistemas.
- La utilización de Internet es para el desempeño de su función y puesto en el FIFONAFE y no para propósitos personales.

4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y password necesarios para acceder a la información y a la infraestructura tecnológica del FIFONAFE, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica del FIFONAFE, debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

4.1 Controles de acceso lógico

4.1.1. El acceso a la infraestructura tecnológica del FIFONAFE para personal externo debe ser autorizado al menos por un Director de área del FIFONAFE, quien deberá notificarlo al Departamento de Desarrollo de Sistemas quien lo habilitará.

4.1.2. Esta prohibido que los usuarios utilicen la infraestructura tecnológica del FIFONAFE para obtener acceso no autorizado a la información u otros sistemas de información del FIFONAFE.

4.1.3. Todos los usuarios de servicios de información son responsables por el UserID y password que recibe para el uso y acceso de los recursos

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Departamento de Desarrollo de Sistemas antes de poder usar la infraestructura tecnológica del FIFONAFE.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del FIFONAFE, a menos que se tenga la autorización del dueño de la información y del Departamento de Desarrollo de Sistemas.

4.1.6. Cada usuario que acceda a la infraestructura tecnológica del FIFONAFE debe contar con un identificador de usuario (UserID) único

y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

4.1.7. Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el UserID de otros usuarios.

4.2 Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del FIFONAFE, deberán ser notificados al Centro de Atención a Usuarios (CAU) con el visto bueno de su Director de área.

4.3 Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como passwords y protectores de pantalla (screensaver) previamente instalados y autorizados por el Departamento de Desarrollo de Sistemas cuando no se encuentren en su lugar de trabajo.

4.4 Administración y uso de Passwords

4.4.1. La asignación del password debe ser realizada de forma individual, por lo que el uso de passwords compartidos está prohibido.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su password, deberá levantar un reporte al Centro de Atención a Usuarios (CAU) para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.

4.4.3. La obtención o cambio de un password debe hacerse de forma segura, el usuario deberá acreditarse ante el CAU como empleado del FIFONAFE.

4.4.4. Esta prohibido que los passwords se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

4.4.5. Sin importar las circunstancias, los passwords nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

4.4.6. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus passwords:

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos.
- Deben ser difíciles de adivinar, esto implica que los passwords no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.
- No deben ser idénticos o similares a passwords que hayan usado previamente.

4.4.7. El password tendrá una vigencia de 90 días, finalizando este periodo el usuario recibe una solicitud electrónica de cambio de contraseña.

4.4.8. Todo usuario que tenga la sospecha de que su password es conocido por otra persona, deberá cambiarlo inmediatamente.

4.4.9. Los usuarios no deben almacenar los passwords en ningún programa o sistema que proporcione esta facilidad.

4.4.10.Los cambios o desbloqueo de passwords solicitados por el usuario al Centro de Atención a Usuarios (CAU) serán notificados con posterioridad por correo electrónico al solicitante con copia al Director de área correspondiente, de tal forma que se pueda detectar y reportar cualquier cambio no solicitado.

4.5 Control de accesos remotos

4.5.1. Esta prohibido el acceso a redes externas vía dial-up, cualquier excepción deberá ser documentada y contar con el visto bueno del Departamento de Desarrollo de Sistemas.

4.5.2. La administración remota de equipos conectados a Internet no esta permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Departamento de Desarrollo de Sistemas.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política

El Departamento de Desarrollo de Sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

5.1 Derechos de propiedad intelectual

5.1.1. Está prohibido por las leyes de derechos de autor y por el FIFONAFE, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por el FIFONAFE.

5.1.2. Los sistemas desarrollados por personal interno o externo que controle el Departamento de Desarrollo de Sistemas son propiedad intelectual del FIFONAFE.

5.2 Revisiones del cumplimiento

5.2.1. El Departamento de Desarrollo de Sistemas realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

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

5.2.3. Los dueños de los procesos establecidos en el FIFONAFE deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

5.3 Violaciones de seguridad Informática

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Departamento de Desarrollo de Sistemas.

5.3.2. Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona

puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Departamento de Desarrollo de Sistemas, con excepción de los Órganos Fiscalizadores.

5.3.3. Ningún usuario del FIFONAFE debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Departamento de Desarrollo de Sistemas.

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

Anexos

Lista de Acrónimos Utilizados

NOMBRE COMPLETO	ACRÓNIMO
Fideicomiso Fondo Nacional de Fomento Ejidal	FIFONAFE
Dirección Administrativa y Financiera	DAF
Departamento de Desarrollo de Sistemas	DDS
Centro de Atención a Usuarios	CAU

Glosario de términos

Es una recopilación de palabras claves que se encuentran en el documento, las cuáles pueden ser términos técnicos, o bien palabras con un significado especial para el proceso definido. Su objetivo es lograr que se maneje un mismo concepto y evitar cualquier tipo de confusión para el correcto entendimiento del documento. Su estructura deberá ser por orden alfabético y la definición de los términos deberá ser clara y breve

Se recomienda marcar en el documento con negritas o en cursiva las palabras claves que puedan causar mayor conflicto para el entendimiento general del proceso.

A	
Término	**Significado**
Acceso.	Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.
Acceso Físico.	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar

	su información.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Aplicación	Acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, Chat, correo electrónico, etc. son algunos ejemplos de aplicaciones en el medio de Internet.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese activo y lograr afectarlo.
Archivo	Una colección identificada de registros relacionados**.**
Autorización	Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.

B	
Base de Datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

C	
CD	Medio de almacenamiento de información.
Código Malicioso	Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.
Comprimir (zip)	Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Zip es el nombre de la extensión que contiene un archivo comprimido.
Computadora	Es un conjunto de dispositivos electrónicos que

	forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.
Confidencialidad	Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.
Correo Electrónico o E-mail	La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar una computadora y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección especifica a través de la red o Internet.
Cuentas de Usuario	Es un identificador, el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

D	
Descargar	Acción de transferir información computarizada de una computadora a otra.
Descomprimir (unzip)	Acción que se lleva a cabo después de haber comprimido un archivo para regresarlo a su estado original.
Discos flexibles (diskettes)	Medios de almacenamiento magnéticos de información de 1.44 Mb llamados comúnmente discos de 3 ½.
Discos Ópticos	Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser, éste al ser reflejado, permite detectar variaciones microscópicas de propiedades “óptico-reflectivas” ocurridas como consecuencia de la grabación realizada en la escritura. Un sistema óptico con lentes encamina el haz luminoso, y lo enfoca como un punto en la capa del disco

	que almacena los datos.
Disponibilidad	Se refiere a que la información esté disponible en el momento que se requiera.
Dominio	Sistema de denominación de host en Internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios Web.

E	
Encripción	Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encripción como tal, no existe en el lenguaje español, el término correcto es cifrado de datos.
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

F	
Falta administrativa	Es la consecuencia que resulta del incumplimiento de la normatividad.
Freeware (Software Libre)	Programas que se pueden bajar desde Internet sin cargo.
FTP	Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red

G	
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

H	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Help Desk / CAU	Soporte técnico brindado a los usuarios telefónicamente, su función es proveer

	conocimientos especializados de los sistemas de producción para identificar y asistir en el ámbito / desarrollo de sistemas y en la resolución de problemas.
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.

I	
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza
Incidente de seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función
Integridad	Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.
Internet o World Wide Web (www)	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo tecnológico.

L	
Lenguaje de Programación	Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.

M	
Maltrato, descuido o negligencia.	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la CNBV.
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el

	impacto en caso de que sea explotada.
Medios Magnéticos (medios de almacenamiento)	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CDs, Cintas, Cartuchos, etc.).
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Metodología	Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente definidas.
Módem	Es un aparato electrónico que se adapta una Terminal o computadora y se conecta a una red de comunicaciones (red telefónica). Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

N	
"Necesidad de saber", principio o base	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.
Nodo	Punto principal en el cual se les da acceso a una red a las terminales o computadoras.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

P	
Página Web	Ver sitio Web.
Parche (patch)	Un parche (algunas veces llamado Fix) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la seguridad o incrementar la

	funcionalidad del mismo.
Password	Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a un computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.

R	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.

S	
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio Web es una lugar virtual en el ambiente de Internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a el.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Software Antivirus	Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.
Switch	Dispositivo de red que filtra y direcciona paquetes a las direcciones destinatarias. El switch opera en la capa de enlace de datos del modelo OSI.

T

Tarjeta Inteligente	Es una tarjeta de plástico del tamaño de una tarjeta de crédito, que incorpora un microchip, en el cual se puede cargar datos como números telefónicos anteriormente llamados, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.

U	
User-ID (identificación de usuario)	Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo (hardware).

V	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.