POLÍTICAS DE USO DE RECURSOS TECNOLÓGICOS

I. OBJETIVO

Proporcionar los lineamientos necesarios para el uso de los diversos recursos tecnológicos con que cuenta la Institución.

II. ALCANCE

Todas las áreas del Pensiones Civiles del Estado de Chihuahua que hacen uso de los recursos tecnológicos con que cuenta la Institución.

III. LINEAMIENTOS

El privilegio del uso de sistemas computarizados y software, así como redes de datos internas y externas, es importante para los empleados de la institución. La preservación de este privilegio para todos los empleados depende de que cada uno cumpla con los estándares externos e internos de uso apropiado de los recursos informáticos, con la finalidad de mantener la disponibilidad de la información en tiempo y forma para todos los usuarios que requieran acceder a esta.

Uso apropiado de los Recursos Tecnológicos

El recurso tecnológico que provee la institución es primariamente utilizado para actividades autorizadas por la misma. El uso del recurso tecnológico está regido por todas las políticas aplicables de la institución, incluyendo, pero no limitándose, a acoso sexual, copyright y políticas disciplinarias de los empleados, así como leyes federales, estatales y locales aplicables.

Uso inapropiado de los Recursos Tecnológicos

La institución califica el uso incorrecto del recurso tecnológico e informático y privilegios como aquellos que resultaren no éticos e inaceptables. El mal uso de los mismos llevará a tomar medidas disciplinarias. El mal uso de los recursos informáticos incluye, pero no se limita, a lo siguiente:

a) Pretender modificar, remover, o agregar accesorios, software, o periféricos sin la apropiada autorización.
b) Acceder a computadoras, software, información computarizada, o redes sin la autorización debida, sin importar que la computadora, software, información o red en cuestión sea propiedad de la institución, incluyendo, pero no limitándose, a abuso o mal uso de las redes que pertenecen a Pensiones Civiles del Estado o computadoras en otros sitios que estén conectadas a esas redes.
c) Traspasar o pretender traspasar límites del uso del recurso, como procedimientos de conexión y regulaciones de seguridad.

d) Enviar correos electrónicos fraudulentos, entrar a casillas de correo ajenas, o leer correos de otros usuarios sin la autorización correspondiente.
e) Enviar cualquier transmisión electrónica fraudulenta, incluyendo, pero no limitándose a pedidos fraudulentos de información confidencial, sumisión fraudulenta de requisitos o recibos de compras electrónicas, autorizaciones fraudulentas de requisitos o recibos de compras.
f) Violar cualquier licencia o copyright de un software, incluyendo copias o distribución de software con licencia, información o reportes sin la autorización apropiada o documentada.
g) Usar recursos informáticos de la institución para acosar o amenazar a otros.
h) Usar recursos informáticos de la institución para el desarrollo, envío o transmisión de cualquiera de los siguientes casos: avisos comerciales o personales, promociones, programas destructivos, material político o religioso, mensajes fraudulentos, acosadores, intimidatorios, profanos, etc. u otro uso no autorizado o personal.
i) Tomar ventaja de negligencia ajena para acceder a cualquier cuenta de red o correo, información, software o archivo que no pertenezca al usuario o para el cual no ha recibido autorización para poder acceder.
j) Interferir físicamente con el acceso de otro usuario al recurso tecnológico (hardware y software) de Pensiones Civiles del Estado.
k) Apoderarse del uso del recurso tecnológico (hardware y software) de otro, incluyendo pero no limitándose, a interrumpir el uso del recurso tecnológico de otros por el uso de video juegos, envió de cadenas de correos electrónicos o cantidad excesiva de mensajes, tanto local como externa; impresión excesiva de documentos, archivos, información o programas; modificación de los sistemas operativos, o partición de discos; pretender sobrecargar computadoras o redes, o dañar computadoras o redes, equipos, software o archivos de las computadoras.
l) Divulgar o remover información, software, impresiones o medios magnéticos sin el explícito permiso del propietario de la misma.
m) Leer información, datos, archivos o programas, sean impresos, desde la pantalla o a través de medios electrónicos sin el explícito permiso del propietario.
n) Violar cualquier ley federal, estatal o local aplicable.

Responsabilidad del usuario

Todos los usuarios de los recursos tecnológicos (hardware y software) de Pensiones Civiles del Estado deben actuar de forma responsable para mantener la integridad de estos recursos.

Todos los usuarios de los recursos tecnológicos propiedad de Pensiones Civiles del Estado, deben respetar el derecho de los otros usuarios.

La política de Pensiones Civiles del Estado es que todos los miembros de la institución actúen de acuerdo con estas responsabilidades, leyes relevantes y obligaciones contractuales y a los más altos estándares de ética.

Protección de contraseñas

Cada usuario es responsable de mantener absoluta seguridad de cualquier contraseña o derecho de contraseña que se le haya asignado. Una contraseña no debe ser compartida con otro usuario, salvo casos de cuentas compartidas en cuyo caso el responsable de las mismas seré el jefe de sección, división o departamento a la que pertenezcan. La protección de las contraseñas ayudará a proteger los sistemas de Pensiones Civiles del Estado de accesos sin autorización.

Respaldos

Es la responsabilidad de los usuarios el asegurarse que información importante e irremplazable de Pensiones Civiles del Estado sea respaldada regularmente. El usuario deberá informarse con el encargado del departamento de sistemas sobre los medios en los cuales puede respaldar la información contenida en su computadora. La información de la institución incluye, pero no está limitada, a documentos de ofimática: (Word, Excel (hojas de trabajo) y presentaciones Power point, bases de datos y reportes.
NO INCLUYE: fotos personales, música, juegos o archivos que no sean para apoyo a su puesto, aunque fueran de ofimática.

Libertad de comunicación

Es la intención de la institución el maximizar la libertad de la comunicación para el cumplimiento de las metas de Pensiones Civiles del Estado. La institución otorga un alto valor a la comunicación abierta de ideas, incluyendo las nuevas y controversiales.
Tanto la institución como los usuarios deben tratar la información guardada electrónicamente en archivos individuales como confidencial y privada. Los contenidos deben ser examinados o divulgados solo cuando el propietario lo autoriza, lo autoriza la institución de forma oficial o es requerida por la ley. La privacidad se ve mitigada en las siguientes circunstancias:

a) Cuando los archivos son generados dentro del proceso de administración de la institución. Los archivos creados o mantenidos por los empleados pueden ser revisados por supervisores dentro del contexto administrativo con ó sin la autorización del usuario.
b) Hay una relación reconocida entre el derecho a la privacidad de la información y la necesidad de los administradores de los sistemas de recopilar la información necesaria para asegurar el funcionamiento continuo de los recursos.

c) En el curso normal de la administración de los sistemas, los administradores pueden supervisar cualquier actividad o examinar actividades, archivos, correos electrónicos y listados de impresora para recopilar la suficiente información para diagnosticar y para corregir problemas con software del sistema o hardware. Los administradores de los sistemas pueden supervisar actividades a archivos para determinarse si se han producido violaciones de la seguridad o si se producirán. En ese caso, el usuario debe ser notificado tan pronto como sea práctico. Los administradores de los sistemas tienen siempre una obligación de mantener la privacidad de los archivos de un usuario, como así también de su correo electrónico y de los registros de su actividad.

Derecho general de privacidad

Los sistemas de aplicación y la información almacenada están sujetos a revisiones por personal autorizado con propósitos de auditoria o cuando se sospeche de la violación de una política de la institución o de alguna ley.

Declaración

La institución no da garantías de ningún tipo, tanto explícito como implícito, con respecto a la comunicación electrónica o servicios que provea. La institución no se hará responsable por ningún tipo de daño sufrido por un usuario por el uso de la comunicación electrónica de la institución o servicios, incluyendo, pero no limitándose, a perdida de información resultado de demoras, falta de envíos, envíos equivocados o interrupción de servicios causados por su propia negligencia o por algún error u omisión de otro usuario. Cualquier información obtenida de Internet será a responsabilidad del propio usuario.

Procedimientos

1. Las cuentas de acceso a recursos informáticos serán entregadas a usuarios autorizados solo por personal de Organización y Sistemas o sus Divisiones.
2. Antes de la entrega de las cuentas y contraseñas, todos los usuarios deben llenar las formas correspondientes, incluyendo las de conocimiento y aceptación de los términos y políticas de la institución.
3. Las contraseñas de los usuarios deben mantenerse en privado y no deben ser entregadas a ningún otro individuo o entidad. Las contraseñas deben ser memorizadas, sin embargo, si una contraseña es escrita, debe quedar resguardada del acceso de otro usuario o entidad. Las contraseñas jamás deben ser puestas en un lugar donde otro usuario pueda verla.
4. La contraseña personal debe ser mantenida por el usuario y debe cambiar periódicamente, o en intervalos más frecuentes como el usuario decida. Las contraseñas deben ser elegidas de acuerdo con las reglas establecidas por el Departamento de Organización y Sistemas.

En el caso de que un usuario conozca la contraseña de otro, la contraseña en cuestión deberá ser cambiada. Cualquier usuario que vea que se hizo un uso desautorizado de su cuenta debe informar inmediatamente al Departamento de Organización y Sistemas.

En el evento de que un usuario aparentemente haga un uso indebido de sus privilegios tecnológicos, o esté involucrado en el mal uso de recursos tecnológicos, entonces la institución puede tomar cualquier o todos los pasos siguientes para proteger a la comunidad de usuarios:

a) Tomar acciones para proteger el sistema, los trabajos de usuarios y archivos de usuarios del daño que se pueda ocasionar.

b) Al empezar una investigación se deberá notificar al Director correspondiente / Jefe del Departamento / Jefe de División / Jefe de Sección /Supervisor inmediato según sea el rango del investigado o del supuesto abusador, que existe una investigación en progreso, argumentando las causas.

c) Referir el tema al área correspondiente según el nivel del investigado dentro de la institución.

d) Suspender o restringir los privilegios tecnológicos del supuesto abusador durante los procesos de investigación y disciplinarios.

e) Inspeccionar los archivos del supuesto abusador, discos compactos, usb u otros medios magnéticos. Los administradores de sistema deben tener causas o evidencias razonables para justificar el acceso a la información del supuesto abusador, antes de inspeccionar los archivos referidos.

f) Si el evento en cuestión también constituye una violación a cualquier ley federal, estatal o local, la institución deberá referir el caso a la Coordinación Jurídica y a su vez a la autoridad pertinente.

Actualización y revisión: 08 de junio del 2023		
Revisó	**Validó**	**Autorizó**
C. Rois Antonio Ramirez Chairez Jefe de la División de Infraestructura y Comunicaciones	**Ing. Francisco Rogelio Rivera Ledezma** Jefe del Departamento de Sistemas	**M.D.O. José Dolores Ramírez Villarreal** Director de Administración