Políticas de Seguridad Informática del DIF Estatal

Elaboró

Lic. Héctor Hugo Ballesteros Hernández

Responsable de Innovación, Desarrollo y Telemática

Revisó

C. José Alberto Morales Matambu

Coordinador de Tecnologías de Información

Aprobó

Licda. Bertha Isabel Cruz López

Coordinadora de Calidad

POLITICAS DE SEGURIDAD

I.- Introducción. -

La Seguridad Informática es un tema de especial relevancia para cualquier persona que tenga contacto con las Tecnologías de Información. Una administración eficiente de los recursos informáticos ayuda a mejorar la Seguridad Informática y la confianza del usuario en los sistemas informáticos sólo se puede lograr a través de una protección efectiva de los diferentes elementos que se integran en las plataformas de cómputo y comunicaciones que sirven para administrar, procesar e intercambiar la información.

Estos ambientes informáticos han sido sometidos a una constante evolución que permanentemente modifica las condiciones de trabajo de los sistemas y genera la aparición de nuevos riesgos y amenazas que deben atenderse para minimizar los efectos potenciales que puedan tener sobre la organización

II.- Glosario. -

Para efectos de las presentes Políticas se entenderá por:

I. **Activos Informáticos:** Comprenden a los recursos informáticos tales como equipos de cómputo, los equipos de Redes, Equipos de Telefonía, el software y las bases de datos.

II. **Autenticación**: Nivel de confianza sobre la identidad del Usuario.

III. **Autorización:** Niveles de Permiso adecuado para establecer acceso a los sistemas, bases de datos o acceso a los servidores.

IV. **Confidencialidad**: Principio de la seguridad de la información que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma,

V. **Desarrollo y Mantenimiento de los Sistemas:** Orientado a garantizar la incorporación de medidas de seguridad en los Sistemas de Información desde su desarrollo hasta su implementación y mantenimiento,

VI. **Disponibilidad**: Principio de la seguridad de la información que garantiza que los Usuarios autorizados tengan acceso a la información o a los recursos relacionados con la misma, toda vez que lo requieran,

VII. **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las Instalaciones de Procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la Institución,

VIII. **Integridad:** Principio de la seguridad de la información que garantiza y salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento,

IX. **Responsable de Desarrollo de Sistemas:** Es el encargado de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información, siguiendo una metodología de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas sus etapas,

X. **Usuario de Sistemas y Servicios:** Al personal de la Institución que haga uso de bienes, servicios, recursos informáticos o de información electrónica que sea responsabilidad del DIF ESTATAL.

III-. Objeto. -

Preservar la integridad, confidencialidad y disponibilidad, así como instrumentar y coordinar acciones para minimizar daños a la infraestructura tecnológica y a los sistemas informáticos.

VI.- Políticas Generales. -

A.- Organización de la Seguridad Informática. -

1.- El objetivo principal será proteger desde el ámbito tecnológico la información electrónica, los recursos informáticos necesarios para que puedan cumplir con las funciones.

2.- La Seguridad Informática implica una responsabilidad a cargo de los Usuario y los del Área de Tecnologías de Información.

3.- La Coordinación de Tecnologías de Información es el área responsable de coordinar acciones, determinar la plataforma tecnológica, y establecer estándares, criterios, medidas y otras disposiciones técnicas, en materia de Seguridad Informática.

POLITICAS DE SEGURIDAD

4.- La Coordinación de Tecnología de Información mantendrá la administración del sistema de autentificación de usuarios que permite el acceso a los recursos y servicios informáticos y de comunicaciones.

La Coordinación de Tecnología de Información dará seguimiento a las medidas específicas en materia de Seguridad Informática que deberán atender los usuarios de los bienes, de los recursos y servicios informáticos y de la información electrónica.

La Coordinación de Tecnología de Información Mantendrá actualizado el inventario de Activos Informáticos relacionados con la Red, Software y Hardware.

La Coordinación de Tecnología de Información Definirá controles de detección y prevención para la protección contra software malicioso.

La Coordinación de Tecnología de Información debe de Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles en la Intranet y en Internet del DIF ESTATAL.

La Coordinación de Tecnología de Información debe de Coordinar los grupos de reacción inmediata y otros grupos de trabajo para manejar los reportes de incidentes y anomalías de Seguridad Informática,

B.- Responsabilidades en Seguridad Informática para el Uso de Bienes, Servicios, Recursos Informáticos y de Información Electrónica. -

1. Todo Usuario tendrá las siguientes responsabilidades:

    a) Atender las medidas de Seguridad Informática que emitida La Coordinación de Tecnología de Información.

    b) Mantener bajo reserva las claves de usuario y los correspondientes códigos de acceso que le hayan sido asignadas.

    c) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas

    d) Bloquear el acceso a su equipo de cómputo cuando deba dejarlo desatendido por algún tiempo,

POLITICAS DE SEGURIDAD

e) Almacenar bajo llave las computadoras portátiles y Memorias USB, en gabinetes u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo, o algún otro medio que evite la sustracción no autorizada de las computadoras portátiles que se encuentren bajo su resguardo,

f) Verificar que las condiciones del lugar donde realiza sus labores sean las adecuadas para evitar que los recursos informáticos y la información bajo su resguardo puedan ser sustraídos por terceros no autorizados y en caso de no contar con las condiciones adecuadas informar a La Coordinación de Tecnología de Información

g) Abstenerse de instalar software sin previa justificación, notificación y autorización.

h) Solicitar a través de email o memos el apoyo para desinstalar el software del que sospeche que tiene una anomalía,

i) Realizar respaldo de la Información Electrónica bajo su responsabilidad para la continuidad de sus funciones,

j) Reportar a la Coordinación de Tecnologías de Información cualquier situación que considere que puede poner en riesgo el Ambiente de Seguridad Informática de la Institución.

2. El uso de recursos del personal o de terceros (Usuarios, Servicio social, Visitas, etc.) para el procesamiento de información en el lugar de trabajo debe ser controlado y autorizado por la Coordinación de Tecnologías de Información al que se destinen los recursos y verificarán que se cumplan medidas propuestas.

3. Todo Usuario que haga uso de equipo de cómputo de la Institución será responsable de su información que genere, así como sus respaldos.

4. Toda persona que desempeñe actividades para apoyar las funciones del DIF ESTATAL y que para sus tareas requiera hacer uso de equipos de cómputo de la Institución, tendrán las siguientes responsabilidades:

a) Establecer las medidas necesarias para proteger la información electrónica que se encuentre bajo su resguardo.

b) No deberán cambiar ninguna configuración del equipo de cómputo sin antes avisar a la Coordinación de Tecnologías de Información.

c) Realizar un respaldo de la Información electrónica bajo su responsabilidad al cambiar de: equipo asignado para el desempeño de sus actividades, de funciones, de área de adscripción o al finalizar su relación con la Institución, y entregarlo de manera formal a su jefe inmediato que haya estado encargado de supervisar sus funciones,

d) Notificar a través de su jefe inmediato cualquier cambio: de equipo, de funciones, o de área de adscripción para que se apliquen las medidas de Seguridad correspondientes,

5. Toda persona que requiera retirar de las instalaciones del DIF ESTATAL algún equipo de cómputo o software deberá contar con la autorización formal de su área administrativa correspondiente, así como el Visto Bueno de la Coordinación de Tecnologías de Información.

6. Toda aplicación desarrollada por la institución o por un tercero debe tener un responsable único designado.

7. Todo Usuario de equipo de cómputo debe de reportar los incidentes de seguridad a su jefe inmediato superior tan pronto hayan tomado conocimiento de su ocurrencia.

8. Los Usuario de Sistemas y equipos de cómputo, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de Seguridad Informática, son responsables de comunicar inmediatamente.

9. El Usuario de equipos de cómputo no debe realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de Seguridad Informática.

10. Todo Usuario de equipos Informáticos que detecte una anomalía de software en producción deberá:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b) Alertar a su jefe inmediato correspondiente.

C.- Seguridad de los Servicios Informáticos. -

1. El Responsable de Desarrollo de Sistemas debe:

POLITICAS DE SEGURIDAD

a) Administrar todos los programas fuentes,

b) Asegurar que todo programa ejecutable en producción tenga un único programa fuente asociado que garantice su origen

c) Asegurar que todo cambio a realizar en el software de aplicación debe efectuarse en el ambiente de desarrollo,

d) Asegurar que para cada cambio realizado en el software de aplicación deben actualizarse los respectivos cambios en el manual de usuario y en la documentación operativa,

e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación,

f) Definir responsables de la Información para cada uno de los ambientes de desarrollo existentes.

g) Verificar que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar los riesgos de fallas de procesamiento y vicios por procesos de errores,

h) Determinar, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados,

i) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios,

j) Evaluar riesgos antes de diseñar la aplicación con el objeto de definir los requerimientos de seguridad e identificar los controles apropiados a aplicar en las etapas del desarrollo de sistemas, prueba de las aplicaciones y ambiente de producción,

k) Identificar y documentar claramente la sensibilidad de la aplicación,

l) Identificar y acordar con el Desarrollador de la Aplicación cuando la aplicación deba de ejecutarse en un ambiente compartido y las aplicaciones con las que compartirá los recursos,

POLITICAS DE SEGURIDAD

m) Implementar controles que aseguren la validez de los datos introducidos,

n) Incluir controles de seguridad y registros con el objeto de evitar la pérdida, modificación o uso inadecuado de los datos en los Sistemas de Información,

o) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operación.

p) Llevar un registro actualizado de todos los programas fuentes en uso, indicando el nombre del programa, programador, analista del programa, versión, fecha de última modificación, fecha / hora de compilación y estado (en modificación, en producción).

q) Respaldar en medios seguros la última, penúltima y antepenúltima versión de los programas fuente y ejecutables, así como su documentación de entorno de cada aplicación como medida de prevención para cualquier contingencia,

r) Toda actualización realizada a las aplicaciones debe ser registrada,

s) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los Usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión,

t) Utilizar técnicas criptográficas apropiadas que permitan la protección de la confidencialidad e integridad de la información cuando se utilice información sensible.

u) Verificar que todo sistema desarrollado e instalado al interior de la Institución y puesto en producción generen registros que contengan excepciones y otros eventos relativos a la seguridad,

v) Verificar que todo cambio a realizar en las aplicaciones sea propuesto por Usuarios de la aplicación.

w) Las demás que determine el Titular de la Coordinación de Tecnologías de Información.

POLITICAS DE SEGURIDAD

2.- El Responsable del Almacenamiento y Respaldo de Información está obligado a:

a) Determinar los requerimientos para resguardar una copia de cada software o dato en función de su criticidad,

b) Disponer y controlar la realización de copias de respaldo,

c) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados y asegurar la destrucción de los medios desechados,

d) Probar periódicamente los medios de resguardo, asegurándose que funcionan correctamente,

e) Retener al menos seis meses de información de resguardo para la información y el software esenciales para la Institución, y

f) Las demás que determine el Titular de la Coordinación de Tecnologías de Información.

3.- El responsable de la gestión de redes debe de:

a) Autenticar las conexiones de nodos de los Sistemas Informáticos,

b) Aprobar accesos a Internet,

c) Verificar y garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución, contra el acceso no autorizado,

d) Asegurar que las conexiones informáticas y los flujos de información no violen los Controles de Acceso.

e) Registrar los accesos de los Usuarios a Internet con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares,

f) Realizar una evaluación de riesgos para la autenticación de usuarios que requieren conexiones externas,

g) Las demás que determine el Titular de la Coordinación de Tecnologías de Información.

POLITICAS DE SEGURIDAD

La aplicación de las políticas de seguridad informática dentro de la institución, nos ofrecen garantías para evitar daños colaterales y preservar la integridad institucional.

Por ello que se recomienda revisar las aplicaciones más usuales, realizar respaldos de la información, no descargar archivos de procedencia desconocida, no utilizar páginas web que no ofrezcan garantías no abrir archivos de remitentes desconocidos, no visitar sitios de contenido ilícito, no utilizar las mismas contraseñas para diferentes páginas, utilizar correos institucionales, no navegar por internet por tiempos prolongados con fines más allá del puro trabajo, descarga ilegal de software, entre otros.

Es conveniente recordar de que estas deben considerarse, es responsabilidad de las y los usuarios la responsabilidad de la información y del uso que les den a los equipos.

Las políticas de seguridad informática atienden análisis de riesgos informáticos que permiten, al mismo tiempo, involucrar a las áreas que poseen los recursos y la experiencia, así como comunicar a todo el personal los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

Las revisiones de las políticas de seguridad informática del DIF Estatal se harán de una forma periódica, para l actualización de las mismas.