LX LEGISLATURA QUERÉTARO

Manual
de Seguridad Informática
del Poder Legislativo de Estado de Querétaro

Fecha de Elaboración:
marzo, 2023
Versión: 02

Contenido

Control de emisión

Elaboró:
Ing. Wilfrido Abel Alvarado Ortiz
Jefe de Tecnologías de la Información y Comunicaciones

Aprobó
Ing. Eduardo Daniel Llamas Romo
Oficial Mayor

Introducción

La información que se genera día a día como parte de las funciones y obligaciones de los órganos, dependencias y unidades del Poder Legislativo del Estado de Querétaro utiliza herramientas tecnológicas que les permiten cumplir en tiempo y forma con cada actividad de trabajo.

Este Poder cuenta con una infraestructura computacional, que soporta su sistema de redes, el cual debe estar en óptimas condiciones para el proceso de generar la información, así como su resguardo y confidencialidad.

La seguridad informática se refiere a los servicios otorgados para resguardar los activos institucionales, tales como los equipos de cómputo, así como la información contenida en los mismos. Estos servicios permiten bloquear cualquier ataque o virus que perjudique la operación institucional.

El presente instrumento normativo es una herramienta que permitirá a los usuarios, conocer las actividades necesarias para la asignación, uso, cuidado, control y aprovechamiento de los bienes y servicios informáticos que proporciona la Oficialía Mayor a través de la Jefatura de Tecnologías de la Información y Comunicaciones, de igual manera, servirá como marco de actuación en esta área, para el óptimo desempeño de sus funciones.

Asimismo, se hace uso de un lenguaje incluyente, con el fin de reafirmar relaciones de respeto e igualdad entre hombres y mujeres en el Poder Legislativo del Estado de Querétaro.

QUERÉTARO
PODER LEGISLATIVO

MARCO JURÍDICO - ADMINISTRATIVO
Constitución Política de los Estados Unidos Mexicanos.
Constitución Política del Estado de Querétaro.
Ley General de Responsabilidades Administrativas.
Ley de Responsabilidades Administrativas del Estado de Querétaro.
Ley de los Trabajadores del Estado de Querétaro.
Ley Orgánica del Poder Legislativo del Estado de Querétaro.

OFICIALÍA MAYOR
DEPARTAMENTO DE TECNOLOGÍAS
DE LA INFORMACIÓN Y COMUNICACIONES

Av. Fray Luis de León No. 2920. Desarrollo Centro Sur.
C.p. 76090. Tel. 442.251.91.00
Santiago de Querétaro, Qro.

www.legislaturaqueretaro.gob.mx

/Legislatura Querétaro
@Legislatura_Qro

Disposiciones Generales

Los Principios de Seguridad en Sistemas de Información se refieren a todas aquellas medidas preventivas que tienen como objetivo proteger la información de un amplio rango de amenazas, así como la creación de estrategias para la elusión de estos. Además, esta se compromete a la preservación de la confidencialidad, integridad y disponibilidad de la información, debido a que la información es un bien que se involucra en todos los niveles económicos e intelectuales de una institución, pues ocupa un lugar en la toma de decisiones y la solución de problemas.

Un Sistema Seguro procura cumplir con los siguientes servicios:

Confidencialidad, para que el acceso a los distintos tipos de recursos, datos e información almacenada sea únicamente para aquellos usuarios que tengan autorización para hacerlo.

Integridad, consiste en asegurar que la información se preserve sin cambios, inalterada, sin pérdida parcial o completa, ante accidentes o ataques maliciosos durante su transmisión a través de una red. De esta forma, se alertan de modificaciones no autorizadas de los datos.

Irrenunciabilidad, este servicio permite comprobar la participación de las partes de un proceso de comunicación. Este es aplicable para aquel que envía el mensaje y quien lo recibe a través de correo institucional u otro medio de comunicación autorizado.

Disponibilidad, que permita que un sistema informático se conserve accesible a los usuarios autorizados cuando estos lo necesiten, al igual que la información. Esto con el objetivo de mantener un sistema robusto de tal manera que soporte ataques e interferencias, y al mismo tiempo se encuentre a disposición de los usuarios que deseen acceder a sus servicios.

Autorización, con el fin de verificar los permisos que corresponden con cada uno de los usuarios, y de esta manera se regula el acceso de los diferentes equipos y servicios del sistema informático, apoyado con mecanismos de autenticación que garantiza que la identidad del usuario es legítima.

Auditabilidad, define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Objetivo

Aplicar las medidas de seguridad informática en los recursos informáticos del Poder Legislativo del Estado de Querétaro.

Alcance

La seguridad informática es responsabilidad de todas y todos los servidores públicos que utilizan los sistemas informáticos: redes, tecnologías y generando información del Poder Legislativo.

La Jefatura de Tecnologías de la Información y Comunicaciones procurará la aplicación de las medidas de seguridad informática, proporcionando el soporte técnico, las asesorías en la materia, así como la difusión de las políticas y protocolos.

El presente Manual contiene recomendaciones en el uso de las tecnologías de la información para su aplicación, que dependerá de la naturaleza de las actividades de los órganos, dependencias y unidades del Poder Legislativo y sujetas a la disponibilidad presupuestal.

Difusión

La Oficialía Mayor a través de la Jefatura de Tecnologías de la Información y Comunicaciones coordinará la difusión del presente Manual.

Medidas de Seguridad Informática:

1.Seguridad Básica.
1.1 Uso de antivirus.
1.2. Asegurar la red.
1.3. Revisión de cuidados con soportes de información externos.
1.4. Actualizaciones de equipos.
1.5. Conexiones seguras.
1.6. Contraseñas seguras.
1.7. Copias de seguridad.
1.8. Información o archivos extraños.
1.9. Protección de Software y Hardware.
1.10. Prevención de incidentes.

2. Seguridad Básica en Internet.
2.1.Acceso a usuarios y utilización de contraseñas.
2.2.Cortafuegos (Firewall).
2.3.Navegadores de Internet.
2.4.Correo Electrónico y Spam.
2.5.Servidores.

3.Seguridad del Usuario
3.1. Malwere.
3.2. Antivirus.
3.3. Sistemas de detección de intrusos.

4.Seguridad de Oficina.
4.1. Seguridad en Wi-Fi.
4.2. Dispositivos fijos y móviles.

5.Confidencialidad.
5.1. Tratamiento de datos personales.
5.2. Navegación en Internet.

1.SEGURIDAD BÁSICA.

1.1.Uso de antivirus. Hacer uso de algún antivirus para evitar, buscar, detectar y eliminar virus de una computadora., cuando se obtenga la información de fuentes externas, como la descarga de archivos y la navegación por la web. Esto es para cualquier tipo de ordenador.

1.2. Asegurar la red. Asegurar la red mediante un firewall para preservar el acceso a la red privada y cifrar la información que se envíe por la red.

1.3. Revisión de cuidados con soportes de información externos. Tener cuidado con dispositivos de almacenamiento externos como son USB, discos duros externos o CD, evitándolos de ser posible, y de ser necesario deben ser analizados por un antivirus antes de utilizarlos, a fin de evitar dispositivos infectados con archivos y o software malicioso.

1.4.Actualización de equipos. Actualizar el equipo, ya sea los sistemas operativos, programas y aplicaciones de manera constante. La Jefatura de Tecnologías de la Información y Comunicaciones elaborará un Programa anual de actualización de equipos, sistemas operativos y las aplicaciones con periodicidad.

1.5. Conexiones Seguras. Utilizar conexiones de internet de confianza, que no pongan en riesgo la seguridad de información. Esto debe de evitarse y de ser necesario utilizar conexiones cifradas con protocolos de HTTPS.

1.6. Contraseñas seguras. La creación de contraseñas debe ser con características seguras, para lo cual se deben aplicar las siguientes medidas:
- Utilizar diferentes contraseñas para cada cuenta que se genere.
- No hacer uso de información personal para las contraseñas.
- Usar el número de caracteres recomendado por la Jefatura de Tecnologías de la Información y Comunicaciones.
- Evitar contraseñas débiles de uso habitual como son "123456", "password", "11111", entre otras.
- Evitar las contraseñas parecidas, en donde se cambia una palabra o carácter.
- Realizar un cambio de contraseña cada año o cuando la cuenta se ha visto vulnerada.
- Evitar compartir contraseñas por correo electrónico o mensaje de texto, así como guardar las mismas en archivos del ordenador.

Las y los Titulares de Dependencias y Unidades aplicarán un mecanismo de resguardo de contraseñas para su recuperación inmediata en caso de pérdidas.

1.7. Copias de Seguridad. (respaldo). La Jefatura de Tecnologías de la Información y Comunicaciones realizará copia de información requeridas por los órganos, dependencias y unidades cuando así lo requieran, y las periódicas que la Jefatura determine.

1.8. Información o archivos extraños. Evitar abrir links o descargar archivos de correos electrónicos extraños y/o páginas de internet. También se puede analizar el correo desde un antivirus. La Jefatura de Tecnologías de la Información y Comunicaciones enviará un recordatorio de esta recomendación de forma periódica por correo electrónico.

1.9. Protección de Software y Hardware.

1.9.1. Software:

1.9.1.1 Antivirus: Programa que impide, protege, busca, detecta y elimina cualquier infección de Malware en dispositivos informáticos, tales como virus, gusanos informáticos, troyanos, entre otros.

1.9.1.2 Cortafuegos: Este va a realizar la función de la primera defensa de seguridad entre una red interna segura e internet (o alguna otra red), su función es controlar el tráfico de red dependiendo de las reglas de seguridad que permita a los usuarios de la red interna, hacer uso de los recursos de internet de manera segura, bloqueando para el acceso a usuarios no autorizados a la red interna.

1.9.1.3 Servicio anti-spam: Estos realizan un filtro automático en el correo para evitar la llegada de correo electrónico no deseado.

Filtros web: *Programas que realizan un filtro sobre las páginas de internet con contenidos inapropiados, se pueden prohibir diferentes categorías de sitios web, además, pueden bloquear el acceso a sitios web que presentan amenaza de malware y se puede bloquear la descarga a ciertos archivos.*

1.9.1.4 Software anti-publicidad: Este impide o elimina todo tipo de anuncios publicitarios, para que los usuarios puedan navegar en internet sin interrupciones y sin posibles amenazas.

1.9.2. Hardware:

1.9.2.1 Protección al acceso físico: Es fundamental colocar mecanismos de prevención de control de accesos y detección contra ataques a un sistema a través de un acceso físico al mismo.

1.9.2.2 Para la prevención se puede utilizar medidas de seguridad como analizadores de retina, tarjetas inteligentes, videocámaras, control de llaves, entre otros. Por otra parte, para la detección, se emplean alertas de acceso denegado o cámaras de vigilancia de circuito cerrado, igualmente las personas que tienen acceso a los equipos pueden detectar cuando un individuo conocido o desconocido se encuentra en sitios inadecuados.

1.9.2.3 Desastres naturales: Se recomienda apoyarse con el área encargada de la Protección Civil para realizar un mapa de riesgos de la infraestructura tecnológica y el análisis del entorno físico, esto para minimizar los daños causados en cualquier catástrofe como son los incendios, tormentas, terremotos, inundaciones, entre otros.

1.9.2.4 Electricidad: Es recomendable el uso de un SAI (Sistema de alimentación interrumpida) para proteger los equipos de problemas derivados del sistema eléctrico que los alimentan, como son los picos de tensión, cortocircuitos, cortes de flujo, entre otros.

1.9.2.5 Protección de datos: Se debe establecer una correcta protección en acceso de forma física de la información almacenada en las copias de seguridad, que incluya el lugar en donde estos van a estar almacenados. Una recomendación para tomar en cuenta es utilizar mecanismos de cifrado, de tal manera que se requiera de clave para acceder a los datos.

1.10. Prevención de incidentes.

1.10.1. Realizar un inventario de todos los activos donde se identifiquen los datos, la información y los sistemas sensibles o críticos para la institución. Se debe proteger, restringir y controlar el acceso a dicho inventario sólo al personal autorizado.

1.10.2. Establecer controles de seguridad física para el centro de procesamiento de datos y de respaldos.

1.10.3. Establecer un monitoreo y control de los accesos remotos e implementar firewalls para el acceso exclusivo de las aplicaciones, servicios, programas y recursos que lo requieran.

1.10.4. Realizar copias de respaldo de seguridad de los dispositivos de red, servidores físicos, servidores virtuales, servicios, accesos de aplicaciones, bases de datos, entre otra información sensible, que puede incluir las siguientes medidas:
- *Establecer procesos y/o procedimientos de respaldo incluyendo la periodicidad.*
- *Realizar pruebas de restauración de las copias de respaldo.*
- *Determinar tiempos de retención de las copias de respaldo.*
- *Almacenar las copias de respaldo en diferentes ubicaciones y medios digitales.*

1.10.5. Segmentar las redes implementando el control de acceso con un firewall para proteger de usuarios no autorizados en las distintas zonas.

1.10.6. Implementar herramientas de análisis de tráfico de red para prevenir y detectar intrusiones o anomalías.

1.10.7. Implementar reglas de filtrados de contenido mediante proxys en la red interna.

1.10.8. Establecer listas blancas de acceso autorizado a sitios web, aplicaciones confiables.

1.10.9. Realizar un fortalecimiento de los servidores para reducción de vulnerabilidades, implementar firewall de host, restringir todos los accesos innecesarios, abrir sólo los puertos requeridos.

1.10.10. Hacer uso de herramientas de bloqueo y prevención, como anti-ransom, filtros antispam, anti-malware, antivirus y bloqueadores JavaScript no confiables.

1.10.11. Establecer políticas de seguridad en los servidores para impedir la ejecución de programas utilizados por el malware.

1.10.12. Priorizar el uso de servidores virtualizados que permitan escalabilidad y disponibilidad.

1.10.13. Utilizar comunicación cifrada entre servidores, aplicaciones y programas.

1.10.14. Implementar protocolos de autenticación segura para identificación y autorización de usuarios en las redes.

1.10.15. Actualizar a las últimas versiones de seguridad más recientes de los sistemas operativos, controladores de software (drivers) y aplicaciones.

1.10.16. Utilizar servidores de correo institucional, evitar utilizar servidores de correo comerciales, configurar el SMTP para que únicamente reciba correo de dominios válidos, para garantizar la recepción de correos con dominios válidos.

1.10.17. Restringir el acceso a servicios web públicos no confiables, mediante filtros de acceso el contenido.

1.10.18. Utilizar contraseñas únicas por cada servidor o software que se administre.

2. SEGURIDAD BÁSICA EN INTERNET.

2.1 Acceso de usuarios y utilización de contraseñas.

2.1.1 Acceso de los usuarios:

Como parte de la seguridad de la institución se toma en cuenta el control de acceso a los usuarios el cual es una herramienta de seguridad, estos permiten la restricción a aquellas personas no autorizadas.

2.1.2 Utilización de contraseñas:

La función principal de las contraseñas es la verificación de la identidad de la persona, por lo que es vital su buen manejo para el resguardo de los datos del usuario, la institución y la red. Los usuarios deben conocer las recomendaciones de seguridad informática para la creación y utilización de las contraseñas.

2.2 Cortafuegos (Firewall).

El firewall es un sistema el cual puede ser por hardware y/o software que ofrece mayor seguridad en la red, debido a que permite filtrar el tráfico de red que entra o sale de acuerdo con la configuración que se realice, esto protege la red de la institución de virus, accesos no autorizados, restricción de páginas, entre otros.

2.3 Navegadores de internet.

En el uso de los navegadores se deben tomar en cuenta diferentes aspectos, tales como:
- Evitar guardar contraseñas.
- Análisis de los complementos instalados
- Cierre las sesiones a las que se ingresa el usuario.
- Actualización constante de los navegadores.

2.4. Correo Electrónico y Spam.

Recomendaciones de seguridad ante el spam malicioso:
- Instalar filtros anti-spam.
- Evitar descargar, o abrir enlaces de correos de origen desconocido.
- Evitar responder a este tipo de correos, o cliclear cualquier tipo de botón o "descripción" que puedan contener.

2.5 Servidores.

Un servidor es un dispositivo de almacenamiento físico o virtual que a través de un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet u otros tipos de redes, LAN, MAN, etc., cuya función es permitir el intercambio de datos entre los diferentes servidores y los equipos de cómputo, garantizando la integridad de la información.

Se recomienda aplicar mecanismos de seguridad en los servidores de la Institución.

3. SEGURIDAD DEL USUARIO

3.1 Malware.

Identificación de malware también llamado software malicioso en los equipos, donde se pueden presentar algunas de las siguientes características en los dispositivos:
- Frecuente despliegue de ventanas emergentes sin autorización.
- Lentitud en el sistema.
- Se deshabilita el antivirus o firewall.
- Problemas en el funcionamiento del dispositivo.
- Modificaciones o eliminación de archivos de manera frecuente.
- Disco duro con alta actividad, aunque el usuario no esté realizando ninguna acción.
- Al conectarse a internet se presentar diversas ventanas del navegador no gestionadas por el usuario.
- Cambio de idiomas de algunos programas.

3.2 Antivirus.

El antivirus es un programa informático, que mediante un escaneo de archivos tiene como objetivo la detección, identificación y eliminación de malware.

Recomendando la actualización constante de los antivirus a cargo del usuario final para una óptima actualización de la base de datos de la que se genera la comparación esto para la protección de nuevas amenazas.

3.3 Sistemas de detección de intrusos.

Uso de un sistema para monitorear de detección de intrusos (IDS) es un programa que monitorea el tráfico de red y las actividades del sistema para de esta forma distinguir los intentos de ataques informáticos a la red, basados en la base de datos de acciones sospechosas sobre una red.

Los beneficios del uso de IDS son los siguientes:
- Prevención de problemas al identificar intentos de accesos no autorizados.
- Otorga una interfaz sencilla de utilizar para cualquier usuario.
- Contiene una base de datos de patrones de actividades maliciosas.
- Identifica violaciones de seguridad y alarma sobre las mismas.
- Ayuda al conocimiento del nivel de riesgo tanto fuera y dentro de la institución.
- Bloquea a los intrusos.

4. SEGURIDAD DE OFICINA.

La seguridad e integridad de acceso físico en la oficina es una parte esencial para la protección de los datos en la institución. Por ende, se debe considerar lo siguiente:
- El control de los accesos.
- Buenas políticas y estructuras adecuadas para proceder en una fuga de información.
- Un correcto mantenimiento del hardware.

4.1 Seguridad en WiFi.

Uso de las diferentes medidas de seguridad para reducir los riesgos del uso de la red inalámbrica, tales como:
- Cambiar las contraseñas predeterminadas
- Control de acceso de los dispositivos conectados a la red por medio de la dirección MAC única de cada equipo.
- Cifrar los datos en la red.
- Uso de diferentes protocolos de encriptación en redes WiFi como WPA, WPA2 y WPA3 que permitan cifrar la información que se transmite entre enrutadores y dispositivos inalámbricos.
- Identificador de conjunto de servicios (SSID).
- Actualizar el software de los puntos de acceso de manera periódica.
- Utilización de una red privada virtual (VPN).

4.2. Dispositivos fijos y móviles.

Máquinas y Dispositivos de Escritorio:

Se recomienda que la Supervisión de Control Patrimonial y la Jefatura de Tecnologías de la Información y Comunicaciones generen una política de uso de los equipos, que encuentre el punto de equilibrio entre la facilidad y flexibilidad en el uso de los dispositivos a cargo del usuario y la seguridad física de estos dispositivos.

Ordenadores Portátiles:

Garantizar la seguridad de los equipos portátiles debido a susceptibilidad de ser robados con facilidad o extraviados. Se recomienda que la Supervisión de Control Patrimonial y la Jefatura de Tecnologías de la Información y Comunicaciones generen una política de uso, control de entrada/salida del centro de trabajo y que además de los dispositivos de escritorio prevean el respaldo de la información.

Redes Privadas Virtuales (VPN):

Dado que la información privada de la organización atraviesa una red pública, esta se hace más vulnerable a ataques informáticos, de eso radica la importancia de la implementación o uso de una VPN para garantizar. mayor seguridad, integridad y confidencialidad a los datos.

5. CONFIDENCIALIDAD.

5.1. Tratamiento de datos personales.

Se sugiere dar cumplimiento a las disposiciones normativas en la materia.

5.2. Navegación en internet.

Las medidas de seguridad informática son las siguientes:
- Navegar por sitios web conocidos.
- Descargar software de sitios oficiales.
- Actualizar constantemente el navegador, de preferencia mantener la versión más actual.
- No aceptar ofertas o descargas sospechosas.
- Preservar el anonimato a medida de lo posible en cuanto a datos personales y/o profesionales en los formularios de petición de datos de sitios web.
- Eliminar con regularidad archivos temporales, cookies e historial de navegación.
- Cambiar contraseñas regularmente.
- Navegar preferentemente en sitios con el protocolo HTTPS.

Glosario de Términos

Acceso remote	Es el medio por el cual el personal usuario realiza una conexión desde una red pública a la red del Poder Legislativo, con la finalidad de hacer uso de los recursos informáticos como Intranet, carpetas de red y sistemas institucionales.
Área solicitante	Órganos, dependencias y unidades de Poder Legislativo del Estado de Querétaro.
Dispositivos de almacenamiento	Todo aquel dispositivo que se utiliza para grabar o leer información digital de un recurso informático de forma permanente o temporal. Recursos informáticos Equipo de cómputo de escritorio o portátil, tabletas, teléfonos IP, impresoras, digitalizadores, programas de cómputo, sistemas de información, aplicaciones, bases de datos y servicios de red. Servicios informáticos Conjunto de infraestructura que proporciona red inalámbrica, mensajería instantánea, correo electrónico, internet, entre otros, que son utilizados por los usuarios del Tribunal Electoral para el desempeño de sus funciones.
Software	Conjunto de programas y rutinas que permiten ejecutar tareas determinadas en un equipo de cómputo.
Software malicioso o malware	Tipo de software, que tiene por objeto infiltrarse al sistema operativo para dañar o robar la información de una computadora sin el consentimiento del usuario.
Usuarios	Personal adscrito a los órganos, dependencias y unidades que hace uso de los recursos o servicios informáticos otorgados por el Poder Legislativo del Estado de Querétaro.
Virus	Software que tiene por objetivo alterar el funcionamiento normal del equipo de cómputo, sin el permiso o conocimiento del usuario, generalmente reemplazan archivos ejecutables por archivos infectados, los cuales pueden destruir intencionalmente datos almacenados.