PROGRAMA DE SEGURIDAD INFORMÁTICA

MUNICIPIO DE TIZAYUCA, HIDALGO

DIRECCION DE INFORMÁTICA Y SISTEMAS

JUNIO 2021

Palacio Municipal S/N Col. Centro, Tizayuca Hgo. C.P. 43800
www.tizayuca.gob.mx

Índice

Introducción

Actualmente la seguridad informática ha adquirido gran auge, aunque no existe en un 100%, ya que por más que tratemos de protegernos instalando algún programa, antivirus o firewall, siempre habrá un atacante tratando de encontrar alguna brecha para sustraer o robar información confidencial de algún lugar específico, aprovechando los recursos disponibles en la web, además cada día se van generando nuevas plataformas, aplicaciones móviles, cloud computing, etc., situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Al día se producen miles de ataques informáticos; las empresas se llevan la peor parte de estos ataques mediante troyanos, virus, gusanos (Worm), Spam, Botnets, Spyware, Keyloggers, Rootkits, puertas traseras (Backdoors), Pishing, Bombas lógicas, Denegación de servicios (DDoS), incluso a través de Ingeniería Social, entre otras, que intentan robar información de los sistemas en los que se instalan.

Cabe mencionar que la información hoy es uno de los activos más importantes con los que cuenta cualquier empresa; aunque no siempre se le tiene la consideración e importancia suficiente. Es necesario hacer ver a las empresas la importancia que tiene la seguridad de su información dentro de sus procesos ya que una pérdida de grandes cantidades de datos, podría llegar a suponer pérdidas millonarias, por eso es importante destacar que podemos tomar ciertas precauciones para minimizar el riesgo como pueden ser ciertas configuraciones correctas con la ayuda de herramientas, tener actualizados nuestros sistemas, analizando y cerrando puertos que no estén en uso.

También existen políticas de seguridad informática que fijan mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Estas políticas deben diseñarse "a medida" para recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el porqué de ello, es decir que pueden tomarse como una forma de comunicación entre los usuarios.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, destreza, experiencia técnica haciendo mención de roles y responsabilidades por cada uno de los integrantes del área, para detectar fallas, debilidades, constancia para renovar y actualizar dichas políticas.

Objetivo general

Definir los lineamientos para promover la planeación, el diseño e implementación de un modelo de seguridad en el Municipio de Tizayuca, Hgo., con la finalidad de garantizar la integridad, disponibilidad y confidencialidad de la información dentro del H. Ayuntamiento.

Alcance

Este documento se aplicará para todos los funcionarios públicos del Municipio de Tizayuca y personal externo que desempeñen labores o proporcionen algún tipo de servicio o producto.

Análisis de problemas identificados dentro del Municipio de Tizayuca

Actualmente dentro del H. Ayuntamiento existen aspectos complejos que recientemente han cobrado un interés central para los responsables de la Subdirección de Informática y Sistemas, que es garantizar la seguridad de la información, así como en la red; la cual tiene como premisa básica permitir el acceso a Internet solo a personal autorizado, al mismo tiempo mantener a los intrusos (hackers, crackers, etc.) fuera de las mismas. Esta tarea se vuelve sumamente difícil cuando los intrusos disponen de información o clave de las redes. Sin embargo, por la falta de lineamientos en materia de seguridad informática y falta de infraestructura, se puede comprometer además de la seguridad de la red, la información que contienen las computadoras del Municipio de Tizayuca, Hgo.

Desde hace tiempo existe información útil donde se incluyen, bases de datos de empleados, información sobre los programas administrativos que se utilizan en las dependencias del Municipio, resultados de licitaciones públicas, etc. Adicionalmente a lo mencionado anteriormente, el hecho de que la Ley de Acceso a la Información Pública y Gubernamental del Estado de Hidalgo, permita que cierta información sea abierta al público, sino es bien identificada, dará acceso a intrusos en la red.

Uno de los elementos que pueden guiar la clasificación de elementos de información cibernética en relación con las redes, es el hecho que, en los equipos usados por los empleados del Municipio de Tizayuca, contienen información de carácter personal, como direcciones (físicas o electrónicas), documentación acerca de su patrimonio tal como: Números y claves de tarjetas de crédito, passwords para acceder a algún sistema, etc.

Otros elementos identificados dentro de la administración pública, es que no existe un sistema de respaldo de información, así como la falta de privacidad de datos, tampoco hay un plan de capacitación para cada uno de los funcionarios donde se les enseñe a realizar un Back Up, evitar descargas que permitan el robo y perdida de datos importantes, infección de virus, spam, ver contenido inapropiado, incluso hasta el mismo cuidado de los equipos de cómputo, todo esto y más, nos hace vulnerables a todo tipo de fallos en cuanto a seguridad.

Roles y Responsabilidades

A continuación, se describen roles involucrados por parte del personal de la Dirección de Informática y Sistemas del Municipio de Tizayuca

Personal Técnico

Rol:

- ✓ Soporte técnico en sitio.
- ✓ Reparación de equipos de cómputo o sistemas pertenecientes al H. Ayuntamiento de Tizayuca, Hgo.
- ✓ Ejecución de mantenimientos preventivos.
- ✓ Elaboración de bitácoras o reportes relacionados con las órdenes de servicio.
- ✓ Asesoría técnica respecto al uso de programas o sistemas.
- ✓ Implementar nuevos proyectos, soluciones y/o ajustes en la infraestructura.
- ✓ Atención a órdenes de servicio.
- ✓ Recepción de requisiciones.
- ✓ Solicitud de consumibles y equipos de cómputo con proveedores.
- ✓ Facturación.
- ✓ Entrega de consumibles y equipos.
- ✓ Actualización y administración de la página web institucional.
- ✓ Responsable de dar solución o buscar alternativas para solventar una problemática.
- ✓ Reportará los eventos de riesgo que sean detectados durante sus horarios laborales.

Director

Rol:

- ✓ Responsable de la adecuada atención a personal del H. Ayuntamiento deTizayuca, Hgo.
- ✓ Relación con funcionarios y proveedores.
- ✓ Atención a nuevas solicitudes de servicios.
- ✓ Informe de estatus de avances de proyectos o servicios.
- ✓ Será el responsable de vigilar que todos los miembros del equipo cumplan con sus actividades, así como ver las necesidades de otras áreas en cuestión de TI.

3. Políticas de seguridad informática a implementar

Estas políticas de seguridad informática que se van a especificar, deben ser muchas de ellas implementadas y revisadas periódicamente, analizando la necesidad de cambios o adaptaciones para cubrir los riesgos existentes, asimismo verificar su cumplimiento.

1. Administración y utilización de antivirus
2. Configuración y utilización de correo electrónico
3. Logueo en equipos de cómputo
4. Acceso a Internet
5. Acceso a la red
6. Acceso y manejo de contraseñas
7. Administración de sistemas
8. Conexión a red inalámbrica
9. Control de acceso a sistemas
10. Control de inventarios de cómputo
11. Escritorio limpio
12. Generación y administración de respaldos
13. Seguridad de la información

14.Seguridad de medios físicos

15.Capacitación

4. Programa de seguridad

A la hora de realizar el análisis del H. Ayuntamiento de Tizayuca, Hgo., se han detectado ciertas vulnerabilidades graves como por ejemplo, que no exista un replicado de la información, que no existan políticas de acceso a la información o la más importante, que la mayoría de los funcionarios no tengan conciencia de la importancia de dotar medidas adecuadas de seguridad para proteger los datos.

Para conseguir reducir el riesgo en cada una de las dependencias que pertenecen al Municipio de Tizayuca, se van a detallar las medidas que se deberán emplear para conseguir ponerse al día en la seguridad de la información y demás elementos informáticos, de esta forma evitar daños y pérdidas.

4.1 Contenido

Este programa presentará las posibles soluciones que debe implementar el H. Ayuntamiento de Tizayuca, Hgo., para conseguir establecer un nivel de seguridad de la información adecuado, con la finalidad de evitar pérdidas y daños en cada una de las dependencias que pertenecen al Municipio de Tizayuca.

Dentro de las medidas que se deben emplear para eliminar las vulnerabilidades y adoptar al H. Ayuntamiento de una seguridad adecuada, se van a distinguir tres tipos:

- Medidas preventivas: Medidas que se deberán implementar para prevenir la posible explotación de una vulnerabilidad por parte de una amenaza, hacker, etc.
- Medidas correctivas: Medidas que se deberán implementar para corregir problemas o fallos de seguridad, debido a amenazas u ataques informáticos.
- Riesgos asumibles: Pueden existir vulnerabilidades que no sean sensibles donde un riesgo las explote, es aquí donde el H. Ayuntamiento aceptará manejar sus propios medios para resolver cualquier inconveniente.

4.1.1 Medidas aplicadas a desastres naturales

Establecer medidas para protegerse de daños por desastres naturales, se debe tomar en cuenta que no se pueden controlar a que lleguen, o no, por lo que el H. Ayuntamiento está expuesto a ellos por muy mínimos que sean, en estos casos únicamente se podrán establecer medidas preventivas para intentar minimizar en lo posible las averías.

Medidas preventivas

- Instalación de dispositivos para protección de líneas eléctricas contra sobrecargas.
- Instalación de dispositivos SAI (Sistemas de Alimentación ininterrumpida), con la finalidad de garantizar el suministro eléctrico en caso de caerse el sistema en general.
- Realización periódica de copias de seguridad (Backup), en cada uno de los equipos de cómputo, servidores y/o sistemas informáticos del Municipio de Tizayuca.

4.1.2 Medidas aplicadas a problemas estructurales

Los posibles daños estructurales, aun siendo ajenos, pueden ser controlados mediante revisiones periódicas o por alguna contratación de servicios alternos.

Medidas preventivas

- ✓ Revisión periódica de la instalación eléctrica.
- ✓ Distribución de extintores cerca de dispositivos o equipos informáticos críticos en las áreas pertenecientes al Municipio de Tizayuca.
- ✓ Contratación de dos líneas suministradoras de Internet, para garantizar siempre una conexión mínima a la red.

Medidas correctivas

- ✓ Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.

Riesgos asumibles

- ✓ Pérdida de comunicaciones durante un periodo inferior a 24 horas.

4.1.3 Medidas aplicadas a problemas de Hardware

Haciendo un análisis dentro del Municipio de Tizayuca y sus respectivas áreas, se han detectado varios fallos en el correcto mantenimiento y seguridad del Hardware disponible, sobre todo debido a la falta de un sistema de almacenamiento, lo que pone en grave riesgo la integridad de la información almacenada en él.

Medidas preventivas

- ✓ Instalar un servidor de almacenamiento centralizado, donde se respalde toda la información generada dentro del Municipio de Tizayuca, asimismo que garantice un acceso adecuado, seguro y que esté disponible a la hora que se requiera.
- ✓ Disponer de copias de respaldo almacenadas en servidores externos, nube computacional, USB, DVD's, discos duros externos, etc., para prevenir posibles fallos de Hardware.
- ✓ Contar con Fuentes de Suministro Eléctrico (UPS), para evitar posibles fallos de los equipos, debido a cortes de energía repentinos.

Medidas correctivas

- ✓ Equipo de soporte técnico y herramienta necesaria, para asegurar una rápida reparación y puesta en marcha de los equipos de cómputo o cualquier dispositivo, en caso de producirse un fallo.
- ✓ Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.

Riesgos asumibles

- ✓ Fallo en alguna estación de trabajo (Equipos de escritorio, Laptop, Servidores, etc.) durante un periodo inferior a 24 horas.

4.1.4 Medidas aplicadas a problemas de Software

Hoy en día el Software es un elemento muy crítico dentro de cualquier empresa, debido a la falta de conciencia de seguridad de los responsables, uno de los motivos principales es la falta de actualizaciones, ocasionando pérdidas de información no deseadas.

Medidas preventivas

- ✓ Realizar periódicamente o cuando sea requerido por el administrador del Software, actualizaciones oportunas para mantener al día los distintos programas y/o Sistemas Operativos.
- ✓ Instalación de bases de datos centralizadas, para almacenar datos importantes generados por el H. Ayuntamiento de Tizayuca, Hgo., facilitando accesibilidad y seguridad de la información.
- ✓ Disponer de Software de calidad y debidamente revisado o auditado.
- ✓ Establecer políticas de contraseñas para acceder a los diferentes equipos del Municipio de Tizayuca.

Medidas correctivas

- ✓ Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.

4.1.5 Medidas aplicadas a problemas de Red

La red es uno de los elementos más sensibles, puesto que dentro de las instalaciones del Municipio de Tizayuca, la mayoría de los servidores públicos, no son conscientes de lo perjudicial que puede llegar a ser un ataque informático externo.

Medidas preventivas

- ■ Montar una red interna para garantizar que todas las comunicaciones y de carácter confidencial no salgan del H. Ayuntamiento, esto con la ayuda de un Firewall para su respectivo monitoreo y administración.

- Mantener correctamente instalados y actualizados los sistemas de seguridad de Software (Antivirus, etc.), en los equipos de cómputo y dispositivos del Municipio de Tizayuca.
- Establecer políticas de seguridad de acceso a la red mediante el uso de contraseñas seguras.
- Instalación de un Router de acceso gestionable, para suministrar la red.
- Configurar adecuadamente la seguridad de red inalámbrica, para evitar accesos no deseados.

Medidas correctivas

- Contar con un correcto servicio de mantenimiento por parte del Carrier que va a suministrar los servicios de comunicaciones, asegurando una rápida reparación y restablecimiento en caso de tener problemas con la línea.
- Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.

Riesgos asumibles

- Fallo en sistemas de comunicación de red durante un periodo no superior a 24 horas.

4.1.6 Medidas aplicadas a problemas con Copias de Seguridad (Backup)

Las copias de seguridad dentro del Municipio de Tizayuca, no se llevan a cabo, ni tampoco se tiene disponible un sistema que garantice el respaldo de datos críticos, ni mucho menos que estos estén a salvo y replicados. .

Medidas preventivas

- Instalación de un servidor de copias de seguridad, en el cual se almacenen periódicamente datos actualizados.
- Fomentar la realización periódica de copias de seguridad de los datos, en especial los críticos, para evitar pérdidas de información importante, de esta forma garantizar la disponibilidad ante cualquier contratiempo dentro de las áreas que pertenecen al Municipio de Tizayuca.

Medidas correctivas

- Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.

4.1.7 Medidas aplicadas a problemas con la Información

La información es uno de los activos más importantes con los que cuenta el Municipio de Tizayuca, uno de los más críticos y los que más se tienen que proteger.

Medidas preventivas

- Disponibilidad de las copias de seguridad de los ficheros más importantes.
- Instalación de base de datos centralizadas, para facilitar el almacenamiento, accesibilidad y seguridad de los datos.
- Crear procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.
- Establecer planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.
- Seguimiento de los procedimientos de seguridad establecidos para cada situación.
- Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.
- Seguimiento del plan de contingencia para cada caso.

4.1.8 Medidas aplicadas a problemas con el Personal

En muchas empresas, el personal es uno de los puntos críticos, ya que un empleado que este en desacuerdo con otros, puede provocar graves daños dentro de las instalaciones, incluso un ataque informático puede surgir dentro de la misma organización.

Medidas preventivas

- ✧ Conseguir una adecuada concienciación de los servidores públicos del Municipio de Tizayuca, sobre lo importante que es mantener un cierto nivel de seguridad en los procesos que se realizan dentro, así como establecer una adecuada política de respaldo de información.
- ✧ Disponibilidad de copias de seguridad.
- ✧ Establecer contraseñas para el acceso a los recursos de los sistemas usados dentro del H. Ayuntamiento.

Medidas correctivas

- ✧ Restauración de copias de seguridad (Backup), en caso de haberse producido una pérdida de datos.
- ✧ Realización de cursos de concienciación sobre la importancia de la seguridad de los datos para el personal del H. Ayuntamiento de Tizayuca, Hgo.

5. Recomendaciones Finales

Una vez realizado el análisis del Municipio de Tizayuca, así como el plan de acciones a implementar, se detallarán algunas recomendaciones, para mantener un nivel y medidas correctas de seguridad informática.

5.1 Recomendaciones

a) Mantener correctamente actualizado todo el software (Antivirus, Sistemas

Operativos, Software de gestión, etc.)

b) Realizar, al menos una vez a la semana, copias de respaldo (Backup) de todos los datos generados en las diferentes áreas del Municipio de Tizayuca.

c) Se recomienda tener personal adecuado, capacitado y actualizado para el mantenimiento de los sistemas y procedimientos de seguridad.

d) Realizar revisiones o auditorias periódicas sobre el nivel de seguridad en que se encuentra el H. Ayuntamiento.