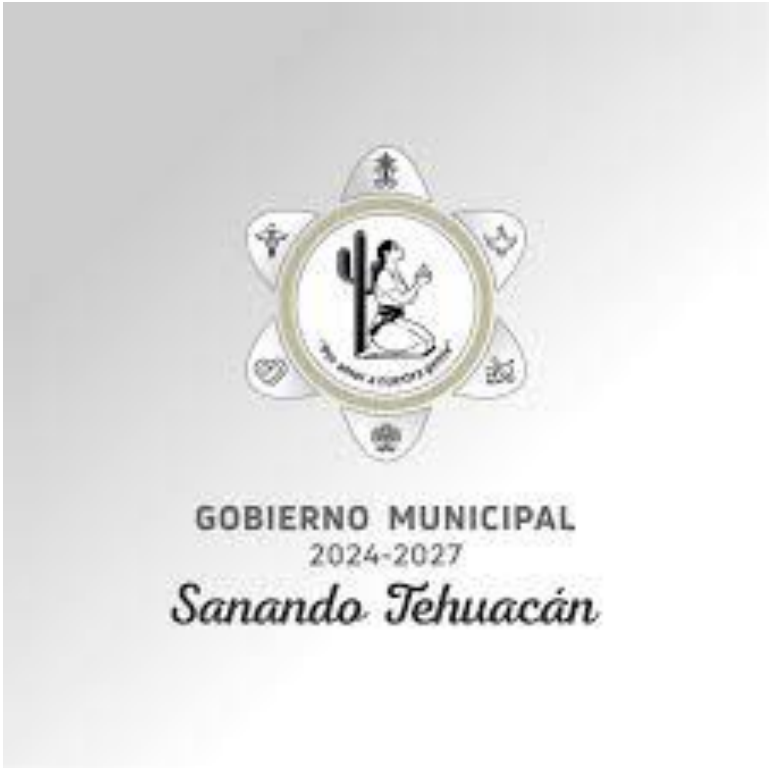
Informe Ejecutivo

Plan Maestro de Ciberseguridad para el Ayuntamiento de Tehuacán



Introducción

Este documento presenta un resumen del Plan Maestro de Ciberseguridad diseñado para el Ayuntamiento de Tehuacán, cuyo propósito es proteger la infraestructura tecnológica, los sistemas críticos y los datos sensibles frente a ciberamenazas. La estrategia considera la evaluación de riesgos, el fortalecimiento de controles de seguridad, y la capacitación del personal, garantizando la continuidad operativa y la confianza en los servicios ofrecidos a la ciudadanía.

Objetivos del Plan Maestro

- Identificar y proteger los activos tecnológicos clave del ayuntamiento.
- Implementar controles de seguridad robustos para mitigar riesgos cibernéticos.
- Diseñar un plan de respuesta ante incidentes que minimice el impacto de ciberataques.
- Promover una cultura de ciberseguridad mediante programas de capacitación y concientización.
- Asegurar la continuidad de las operaciones críticas en caso de interrupciones.

Áreas de Enfoque

1. **Inventario de activos tecnológicos:**
- Identificación de sistemas y áreas críticas como Coordinación de Informática y Sistemas, Contraloría Municipal, Transparencia, Registro Civil y Obras Públicas, entre otras.
- Clasificación de activos según su nivel de importancia y sensibilidad.
2. **Topología de red y segmentación:**
- Diseño de una red segmentada para proteger los sistemas más críticos.
- Implementación de firewalls y configuración de medidas de seguridad en los puertos de red.
3. **Políticas de seguridad:**
- Establecimiento de normas básicas de seguridad, como la actualización de sistemas, gestión de contraseñas seguras y control de accesos.
- Revisión periódica de logs para detectar actividades sospechosas.
4. **Gestión de incidentes:**
- Creación de un plan de respuesta a incidentes con procedimientos claros para detección, contención, mitigación y recuperación.
- Formación de un equipo dedicado a la gestión y análisis de incidentes de seguridad.
5. **Capacitación y concientización:**
- Programas de sensibilización dirigidos a los empleados sobre riesgos como el phishing, el malware y el uso seguro de las tecnologías.

Metodología

El plan se desarrolló en varias etapas clave:

Evaluación inicial de riesgos para identificar vulnerabilidades y áreas prioritarias.

- Este proceso tiene como objetivo identificar, analizar y gestionar los riesgos potenciales que pueden amenazar la seguridad de la información y los activos tecnológicos del ayuntamiento.

Sistemas Operativos Encontrados	No. De Equipos
Windows Server 2003 SP2	36 equipos
Windows (sin especificar versión)	1 equipo
Windows 7 SP1:	2 equipos
MikroTik RouterOS versión 6.45.6	1 equipo

Cantidad de computadoras por nivel de riesgo	
Riesgo Alto **(26 equipos)**	Puertos comunes: 445/tcp (SMB), 3389/tcp (RDP), 1433/tcp (SQL Server), 135/tcp (DCE/RPC). Vulnerabilidades críticas relacionadas con software obsoleto o sin soporte.
Riesgo Medio **(8 equipos)**	Puertos comunes: 135/tcp, 49664/tcp, general/icmp. Vulnerabilidades menos críticas, pero aún con exposición a ataques.
Riesgo Bajo **(6 equipos)**	Puertos comunes: generales (TCP Timestamps, icmp). Vulnerabilidades menores, con bajo riesgo de explotación.

Diseño de estrategias de protección adaptadas a las necesidades del ayuntamiento.

1. **Nuevos controles de acceso**

a) Política de Contraseñas Robusta

- Requisitos de Contraseña: Longitud mínima de 8-12 caracteres.
- Complejidad: Incluir mayúsculas, minúsculas, números y símbolos.
- Restricciones: No usar información personal (nombres, fechas de nacimiento).
- Cambio Regular de Contraseñas:
- Frecuencia: Cambiar contraseñas cada 3-6 meses.
- No Reutilizar: Evitar el uso de contraseñas previamente utilizadas.
- Uso de Gestores de Contraseñas:
- Recomendado para almacenar y generar contraseñas seguras, ayudando a mantener contraseñas únicas para cada cuenta.

b) Autenticación de Dos Factores

- Definición: Método que requiere dos formas de verificación para acceder a una cuenta, proporcionando una capa adicional de seguridad.

- Métodos de Autenticación: Código SMS o Correo Electrónico: Recibir un código en el móvil o email que debe ingresarse junto con la contraseña.
- Aplicaciones de Autenticación: Utilizar aplicaciones como Google Authenticator o Authy para generar códigos de acceso temporales.
- Beneficios de la 2FA: Mayor Seguridad: Aumenta la protección contra accesos no autorizados y reduce el riesgo de que las credenciales sean comprometidas.
- Protección contra Amenazas: Disminuye el impacto de ataques de phishing y fuerza bruta al requerir una verificación adicional.

2. Actualización Y Parcheo De Sistemas

a) Vulnerabilidades Detectadas y Análisis
   - Windows Server 2003 en varios hosts, como 192.168. ***.***.
   - phpMyAdmin 2.10.3 en el puerto 8080/tcp, una versión descontinuada.
   - Apache HTTP Server 2.2.8 también en el puerto 8080/tcp.
   - PHP versión 6.0.0, que es vulnerable y desactualizada, en varios servicios.
   - Vulnerabilidades de Ejecución Remota de Código (RCE): Problemas críticos como la vulnerabilidad de "BlueKeep" (CVE-2019-0708) en el servicio RDP (3389/tcp), que permite a los atacantes ejecutar código de forma remota sin autenticación.

b) Recomendaciones para Actualización y Parcheo
   - Sistemas Operativos:
     Actualizar todos los hosts con Windows Server 2003 a versiones soportadas, como Windows Server 2019 o 2022.
   - phpMyAdmin:
     Actualizar la versión de phpMyAdmin a la más reciente (recomendada 5.x), para corregir los problemas de seguridad.
   - Apache HTTP Server:
     Migrar a Apache versión 2.4.58 o superior, ya que ofrece soporte y parches para vulnerabilidades recientes.
   - PHP:
     Actualizar PHP a la versión 8.1.30 o superior, como 8.2.24 o 8.3.12, para cerrar múltiples vulnerabilidades críticas de seguridad.

3. Protección de Red y Datos

a) Configurar medidas de seguridad de red básica
   - Configurar políticas de firewall: Establecer reglas claras para permitir solo el tráfico necesario y bloquear accesos no autorizados, enfocándose en puertos y protocolos específicos.
   - Firewalls de próxima generación (NGFW): Estos permiten detectar y bloquear amenazas avanzadas, y pueden configurarse para analizar el tráfico a nivel de aplicación.
   - Actualización continua: Mantener el firmware y las políticas del firewall al día para mitigar vulnerabilidades.

b) Seguridad en puertos de red
   - Deshabilitar puertos no utilizados: Cerrar puertos en switches y routers para evitar accesos no autorizados.

- Monitoreo y alertas de puertos: Configurar alertas de actividad inusual en puertos de red, lo que permite detectar posibles accesos indebidos.
- Control de acceso a puertos físicos: Asegurarse de que los puertos de red físicos en ubicaciones accesibles al público estén protegidos o, de ser posible, inhabilitados.

c) Verificar y probar las copias:
   - Realizar pruebas de recuperación periódicas y verificar automáticamente las copias para asegurar que puedan restaurarse sin problemas en caso de emergencia. Además, configurar alertas para fallos en el proceso de respaldo.

d) Documentación y capacitación:
   - Documentar los procedimientos y políticas de respaldo, e incluir sesiones de capacitación para el personal encargado, de manera que sepan cómo proceder ante una recuperación de datos.

Implementación de herramientas tecnológicas para el monitoreo y la prevención de amenazas.

Establecer un Sistema de Copias de Seguridad

- Identificar datos críticos que requieren respaldo.

Área Critica	Tipos de Datos	Frecuencia de Respaldo	Método de Respaldo	Frecuencia de Verificación
Contraloría Municipal	Informes financieros, auditorías, contratos	**Diario**	**Completo e incremental**	**Trimestral**
Desarrollo Urbano	Planos de zonificación, permisos	**Semanal**	**Incremental**	**Trimestral**
Desarrollo Económico	Programas de incentivos, proyectos de inversión	**Semanal**	**Incremental**	**Trimestral**
Fomento Comercial y Abasto	Licencias comerciales, regulaciones	**Semanal**	**Incremental**	**Trimestral**
Ingresos	Registros de pagos, facturas, impuestos	**Diario**	**Completo e incremental**	**Mensual**
Registro Civil	Actas de nacimiento, matrimonio, defunciones	**Diario**	**Completo e incremental**	**Mensual**
Obras Públicas	Proyectos de obra, presupuestos, cronogramas	**Semanal**	**Incremental**	**Trimestral**

Frecuencia de Respaldo: Determina cada cuánto tiempo se realiza el respaldo de los datos.

Método de Respaldo: Uso de métodos completos (copia de todos los datos) e incrementales (copia solo de los cambios recientes).

Frecuencia de Verificación: Periodicidad con la que se realizan pruebas de restauración para verificar la integridad de los datos respaldados.

- Implementar un proceso de copias de seguridad regulares y verificar su funcionamiento.

Pasos	Descripción	Herramientas Recomendadas
1.Configuración del Respaldo	Definir la configuración de respaldo y la frecuencia de copias (diaria, semanal, mensual) para cada área.	Veeam, Acronis, Bacula, Duplicati
2. Automatización	Programar respaldos completos e incrementales automáticamente, según la frecuencia de cada área crítica.	Veeam (tiene opciones de automatización), Acronis, Windows Backup, Restic
3.Monitoreo y Notificaciones	Activar alertas automáticas para errores o fallos en los respaldos, y llevar un registro de cada respaldo.	Veeam Monitor, Nagios, Zabbix, Acronis
4. Pruebas de Restauración	Realizar pruebas regulares de restauración para verificar la integridad de los datos respaldados.	Veeam Recovery, Acronis Disaster Recovery, Windows Backup Restore
5. Documentación	Documentar los procedimientos de respaldo, configuraciones y procesos de restauración.	Confluence (para documentar procesos), Notion, Microsoft OneNote
6. Auditorías y Evaluación	Realizar auditorías periódicas y evaluar la tecnología de respaldo según las necesidades del ayuntamiento.	Excel (para auditorías manuales), Veeam Reports, Power BI

Plan de Respuestas a Incidentes

El plan de respuesta a incidentes es fundamental para mitigar los efectos de los incidentes de seguridad en el ayuntamiento. Incluye:

- Detección y Clasificación: Uso de herramientas de monitoreo y sistemas de clasificación para identificar y categorizar amenazas.
- Respuesta Eficaz: Protocolos claros para la contención, eliminación y recuperación.
- Equipo de Respuesta a Incidentes (ERI): Conformado por roles especializados en seguridad, administración de redes y comunicación para gestionar incidentes de manera rápida y eficiente.

Esta tabla ayudará a presentar los puntos clave del plan de respuesta a incidentes de forma clara y estructurada.

Elemento	Descripción	Herramientas Propuestas
Detección de Incidentes	Identificar y alertar sobre actividades inusuales, accesos no autorizados o vulnerabilidades activas.	IDS/IPS: Snort, Suricata SIEM: Splunk, AlienVault
Clasificación de Incidentes	Categorizar los incidentes según su severidad (bajo, medio, alto, crítico) y su tipo (amenaza interna, externa, malware, etc.).	SIEM para clasificación automatizada Herramientas de análisis de logs
Respuesta a Incidentes	Protocolo para contener, eliminar y recuperar sistemas tras un incidente (ej. aislamiento de sistema infectado, análisis de malware, restauración de datos).	Antivirus: CrowdStrike, Symantec Backup: servidores dedicados para copias de seguridad
Equipo de Respuesta a Incidentes (ERI)	Establecimiento de un equipo de respuesta con roles asignados para actuar de inmediato ante incidentes.	Documentación y comunicación interna Herramientas de comunicación (ej. Microsoft Teams, Slack)
Roles Clave en el ERI	Responsable de Respuesta a Incidentes: Coordina y toma decisiones críticas. Analista de Seguridad: Analiza la causa y colabora en la contención. Administrador de Redes: Implementa las medidas de recuperación. Comunicador de Incidentes: Informa a la dirección y usuarios.	Gestión de roles: Sistema de asignación de tareas Comunicación y reportes

Implementar Monitoreo Básico de Seguridad

- Configurar herramientas de monitoreo que detecten actividad sospechosa.
- Establecer un sistema centralizado para gestionar alertas de seguridad.
- Definir procesos para el monitoreo en tiempo real de los sistemas críticos.

Actividad	Descripción	Responsable	Frecuencia
Configuración de monitoreo	Implementar herramientas básicas como SIEM o logs centralizados.	Equipo de TI	Una vez
Revisión de eventos	Analizar logs para identificar actividades inusuales.	Equipo de Seguridad	Diario
Respuesta a incidentes	Notificar y resolver incidentes detectados en el monitoreo.	Equipo de Incidentes	Según sea necesario

Configurar Alertas de Seguridad en Sistemas Críticos

- Establecer reglas de alertas para actividades específicas (por ejemplo, intentos de acceso no autorizado).
- Clasificar alertas según su prioridad (baja, media, alta).
- Garantizar la notificación inmediata a responsables relevantes.

Sistema Crítico	Tipo de Alerta Configurada	Prioridad	Acción Requerida
Servidores de datos	Acceso no autorizado	Alta	Bloquear y notificar
Red de comunicaciones	Tráfico inusual	Media	Investigar
Aplicaciones municipales	Fallos repetidos de autenticación	Alta	Desactivar cuentas

Establecer un Proceso de Revisión Diaria de Logs

- Revisar diariamente los registros de los sistemas críticos.
- Documentar hallazgos y acciones tomadas.
- Utilizar herramientas automatizadas para destacar anomalías importantes.

Actividad	Descripción	Herramienta	Frecuencia
Revisión de logs críticos	Analizar eventos recientes.	Syslog, Splunk	Diario
Generación de reportes	Resumir actividades y alertas.	Dashboard SIEM	Diario
Escalamiento de incidentes	Notificar problemas a responsables.	Correo o ticketing	Según hallazgo

Revisión constante y ajustes según las tendencias de seguridad actuales.

Evaluación y Planificación Futura

- Realizar una evaluación periódica para medir el progreso de las medidas implementadas.
- Identificar debilidades en el sistema actual y priorizar mejoras.
- Diseñar un plan futuro basado en tecnologías emergentes y nuevas amenazas.

Aspecto Evaluado	Resultados Esperados	Medida Correctiva (si aplica)
Efectividad de las alertas	Detección oportuna de incidentes	Ajustar reglas de alertas
Cobertura de monitoreo	Inclusión de todos los sistemas críticos	Ampliar monitoreo a nuevos sistemas
Capacitación del personal	Manejo efectivo de herramientas de seguridad	Realizar entrenamientos adicionales

Plan Futuro:

Prioridad	Acción	Tiempo Estimado
Alta	Migrar a soluciones avanzadas de SIEM.	Próximos 6 meses
Media	Automatizar revisiones de logs.	Próximo año
Baja	Explorar inteligencia artificial para predicción de amenazas.	A 2 años

Resultados Esperados

- Reducción de las vulnerabilidades identificadas en las áreas críticas.
- Incremento en la capacidad de respuesta ante eventos de seguridad.
- Mayor concientización del personal sobre la importancia de la ciberseguridad.
- Protección reforzada de la información sensible y los sistemas críticos del ayuntamiento.

Beneficios a Largo Plazo

- Resiliencia operativa frente a ciberataques y desastres tecnológicos.
- Cumplimiento de normativas legales aplicables a la gestión de datos y seguridad.
- Mejora de la confianza de los ciudadanos en los servicios digitales del ayuntamiento.

Conclusión y Siguientes Pasos

- El Plan Maestro de Ciberseguridad es un paso decisivo para fortalecer la protección de los sistemas del ayuntamiento. Para garantizar su efectividad, se recomienda:
- Realizar auditorías de seguridad periódicas.
- Actualizar las herramientas y políticas de ciberseguridad conforme a las nuevas amenazas.
- Mantener un enfoque constante en la capacitación y sensibilización del personal.

Producto de Éxito

Durante mi colaboración con el Ayuntamiento de Tehuacán, lideré la implementación del Plan Maestro de Ciberseguridad, desarrollado a través de mi empresa CYBERWALL TEHUACAN. Este proyecto fue diseñado para fortalecer la seguridad de la infraestructura tecnológica del ayuntamiento mediante medidas como la actualización de sistemas, la implementación de políticas de seguridad y la definición de un plan de respuesta a incidentes.

El equipo de CYBERWALL TEHUACAN, conformado por Diana Luz Contreras Guzman, Jony Alonso Zeferino, David Hilam Reyes Herrera, Lucio Armando Villarreal Lopez, Angel Jesus Rodríguez Sanchez trabajó de manera eficiente para garantizar la conclusión exitosa del proyecto.

Este plan ha sido entregado oficialmente y está dirigido al **Ingeniero Edgar Uriel Sanpedro Sánchez, Coordinador de Informática y Sistemas, y al Ingeniero Julio César Muñoz Méndez**.

Estado del Proyecto: Concluido exitosamente