Resumen, hallazgos y recomendaciones del SGSI para USPS

4Geeks

- Nombre: **Luciano Matias Zuccardi**

- Fecha: **10 de febrero de 2025**

Introduccion

Importancia de la Ciberseguridad para el USPS:

- Infraestructura crítica y gran volumen de datos
- Confianza del público y cumplimiento normativo
- Riesgos y amenazas actuales (ej: ransomware, phishing, etc.)

Objetivos del SGSI:

- Proteger la confidencialidad, integridad y disponibilidad de la información
- Garantizar la continuidad de las operaciones
- Cumplir con leyes y regulaciones

Metodología

Enfoque del SGSI:

- Basado en estándares y mejores prácticas (ej: NIST CSF, ISO 27001)
- Adaptado a las necesidades específicas del USPS
- Análisis de riesgos y evaluación de vulnerabilidades

Proceso de Implementación:

- Fases del proyecto (ej: planificación, diseño, implementación, etc.)
- Colaboración con equipos internos del USPS
- Herramientas y tecnologías utilizadas

Hallazgos Clave, de amenazas, vulnerabilidades e impactos.

AMENAZAS	Vulnerabilidad Potencial	Impacto Potencial
Ataque de denegación de servicio (DoS)	Falta de protección contra ataques volumétricos (ej: SYN flood, UDP flood).	El sitio web queda inaccesible para los usuarios, impidiendo la compra de sellos y el seguimiento de envíos.
Acceso no autorizado	Vulnerabilidades en el software del servidor web (ej: errores de configuración, software sin parches).	Un atacante accede a la base de datos de usuarios y roba información personal de clientes.
Desastres naturales (incendios, inundaciones)	Falta de un plan de recuperación ante desastres robusto, ubicación vulnerable del centro de datos.	Un incendio destruye el centro de datos principal, perdiendo información crítica y dejando a la USPS sin capacidad operativa.
Acceso físico no autorizado	Falta de medidas de seguridad física (ej: control de acceso deficiente, cámaras de seguridad insuficientes).	Un intruso roba equipos con información confidencial de clientes y empleados.
Ingeniería social (phishing)	Falta de capacitación, políticas de contraseñas débiles.	Un empleado revela sus credenciales de acceso a un atacante, permitiéndole acceder a sistemas internos y robar información.
Filtración de datos	Clientes: • Falta de cifrado de datos sensibles, controles de acceso insuficientes. Terceros: • Falta de contratos con cláusulas de seguridad robustas, falta de auditorías de seguridad a terceros.	Clientes: Un atacante accede a la base de datos y roba información personal de millones de clientes. Terceros: Un proveedor de servicios sufre una brecha de seguridad exponiendo información de clientes de USPS.
Manipulación de datos	Falta de validación de datos en la aplicación web, falta de integridad en la base de datos.	Un empleado malicioso modifica la información de seguimiento de un paquete y lo desvía para robar su contenido.
Ransomware	Falta de copias de seguridad actualizadas, falta de segmentación de la red.	Un ataque de ransomware cifra los sistemas de seguimiento, impidiendo el acceso a la información y exigiendo un rescate.

Recomendaciones y respuestas a posibles amenazas

Amenaza	Controles y mitigaciones	Roles y Responsabilidades
Ataque de Denegación de Servicio (DoS)	Firewall con reglas de filtrado avanzadas.	Equipo de Seguridad de Red. Administrador de Firewall.
	Sistema de Detección y Prevención de Intrusiones (IDPS).	Equipo de Seguridad de Red. Analista de seguridad
	Análisis de vulnerabilidades y pruebas de penetración.	Equipo de Seguridad de Aplicaciones. Analista de Seguridad.
Acceso No Autorizado a Servidores Web	Políticas de contraseñas robustas.	Equipo de Seguridad. Administrador de Sistemas.
	Autenticación de dos factores.	Administrador de Identidad y Acceso. Equipo de Seguridad.
	Control de acceso basado en roles.	Administrador de Identidad y Acceso. Equipo de Seguridad.
Pérdida de Datos por Desastres Naturales	Plan de recuperación ante desastres detallado.	Equipo de Continuidad de Negocio. Equipo de Operaciones de TI.
	Sitio de respaldo o replicación de datos.	Arquitecto de Infraestructura. Administrador de Sistemas.
Filtración de Datos a través de Terceros	Evaluación de riesgos de seguridad de terceros.	Equipo de Seguridad. Oficial de Cumplimiento.
	Contratos con cláusulas de seguridad detalladas.	Departamento Legal. Equipo de Seguridad.
	Auditorías de seguridad periódicas a terceros.	Auditor Interno. Equipo de Seguridad.