Resultados de la evaluacion de riesgos para USPS

1 - Identificación de los riesgos asociados con la Organización y sus Activos.

ACTIVO	CLASIFICACIÓN	RIESGOS ASOCIADOS
Bases de datos de clientes	**Critico**	La pérdida o divulgación de esta información tendría un impacto catastrófico en la reputación del USPS, la confianza del cliente y podría generar sanciones legales.
Software de seguimiento de envíos	**Critico**	La interrupción de este sistema afectaría gravemente la capacidad del USPS para operar y cumplir con sus obligaciones de entrega.
Servidores (físicos y virtuales)	**Alto**	Estos servidores alojan las aplicaciones y datos críticos para el negocio. Su interrupción tendría un impacto significativo en las operaciones.
Equipos de red (routers, switches)	**Alto**	La caída de estos equipos afectaría la conectividad y disponibilidad de los sistemas críticos.
Información de clientes (Nombres, direcciones)	**Alto**	Esta información también reside en otros sistemas y documentos. Su protección es fundamental para la privacidad del cliente.
Datos de envío (seguimiento de paquetes)	**Medio**	La interrupción temporal de este acceso a los datos de envío no tendría un impacto tan grave como la pérdida de la base de datos de clientes
Información financiera	**Medio**	La información financiera es sensible, pero su impacto en las operaciones diarias es menor en comparación con los activos críticos.
Registros de empleados	**Medio**	Esta información es confidencial y debe protegerse, pero su impacto en las operaciones es moderado.
Computadoras de escritorio y portátiles	**Bajo**	Su pérdida individual no tendría un impacto significativo en las operaciones generales del USPS.
Dispositivos móviles	**Bajo**	Similar a los equipos de escritorio, la pérdida individual de dispositivos móviles tendría un impacto limitado.
Sistemas operativos	**Bajo**	Aunque son necesarios, los sistemas operativos son genéricos y pueden reinstalarse en caso de fallo.

2 - Identificación y probabilidades de potenciales amenazas.

ACTIVO	TIPO DE ACTIVO	AMENAZAS	DESCRIPCIÓN	PROBABILIDAD
Sitio web publico (usps.com)	**web**	Ataque de denegación de servicio (DoS)	Interrupción del acceso al sitio web, afectando la disponibilidad de servicios para los usuarios.	**Media**
	Infraestructura web	Acceso no autorizado	Intrusión a servidores web, robo de datos o modificación del sitio web.	**Baja**
Centros de datos	**Infraestructura**	Desastres naturales (incendios, inundaciones)	Pérdida total o parcial de datos e infraestructura, interrupción de servicios.	**Baja**
		Acceso físico no autorizado	Intrusión física a centros de datos, robo de equipos o acceso a información sensible.	**Baja**
Empleados	**Usuarios**	Ingeniería social (phishing)	Manipulación para revelar información confidencial o credenciales de acceso.	**Alta**
Terceros (proveedores, partners)	**Terceros**	Filtración de datos	Acceso no autorizado a información de USPS a través de terceros.	**Baja**
Datos de clientes	**Servidores de Datos**	Filtración de datos	Exposición de información personal de clientes, robo de identidad, pérdida de confianza.	**Media**
Sistemas de seguimiento de paquetes	**Aplicacion web / Base de datos**	Manipulación de datos	Alteración de información de seguimiento, robo de paquetes, fraude.	**Baja**
		Ransomware	Secuestro de sistemas y datos, extorsión para recuperar el acceso.	**Media**

3. Evaluación de vulnerabilidades y su impacto

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.

4. Clasificación de Riesgos de activos según criterios CID

La evaluación de riesgos basada en los criterios CID permite analizar de forma estructurada las amenazas y vulnerabilidades que pueden afectar a los activos de información, facilitando la toma de decisiones informadas para su protección.

- **Confidencialidad:** Protección de la información sensible contra accesos no autorizados.
- **Integridad:** Garantía de que la información se mantiene precisa y completa, sin modificaciones no autorizadas.
- **Disponibilidad:** Asegurar que la información esté accesible para los usuarios autorizados cuando la necesiten.

CATEGORIA	Confidencialidad	Integridad	Disponibilidad
Sistemas de Infraestructura critica	**Muy alto**	**Muy alto**	**Muy alto**
Información Financiera	**Muy alto**	**Muy alto**	**Alto**
Información del Cliente	**Alto**	**Alto**	**Alto**
Información de Empleados	**Alto**	**Alto**	**Medio**
Comunicaciones Internas	**Medio**	**Alto**	**Alto**
Datos de Envíos	**Medio**	**Alto**	**Alto**
Planes de Operacion	**Alto**	**Alto**	**Bajo**
Documentación Legal	**Alto**	**Alto**	**Bajo**