TOPCERTIFIER
www.topcertifier.com

METODOLOGÍA DEL SERVICIO PCI DSS

Estándar de seguridad de datos de la industria de tarjetas de pago.

TOPCERTIFIER
www.topcertifier.com

INTRODUCCIÓN PCI DSS

TOPCertifier presenta una lista de verificación de análisis de brechas PCI DSS simplificada para ayudarlo a identificar áreas donde su organización puede necesitar mejoras para cumplir con PCI DSS (Pago Estándar de seguridad de datos de la industria de tarjetas). Esta lista de verificación ofrece una base marco para evaluar su alineación con PCI DSS y sirve como paso inicial en evaluar su cumplimiento.

SECCIÓN 1: SEGURIDAD DE LOS DATOS

- Los datos de la tarjeta de pago están correctamente cifrados durante la transmisión y el almacenamiento
- Los datos de autenticación confidenciales, como los números CVV, no se almacenan después de la autorización
- Existe una política para proteger los datos del titular de la tarjeta y los datos de autenticación confidenciales

SECCIÓN 2: SEGURIDAD DE LA RED Y DEL FIREWALL

- Se revisan y actualizan periódicamente las configuraciones de red y las reglas del firewall
- Existe un diagrama de red que ilustre el flujo de datos de los titulares de tarjetas
- Existen políticas y procedimientos de seguridad para proteger la infraestructura de red

SECCIÓN 3: CONTROL DE ACCESO

- Están restringidos los privilegios de acceso de los usuarios según la necesidad de conocimiento empresarial
- Se implementa la autenticación multifactor para el acceso remoto a la red
- Las cuentas de usuario se desactivan rápidamente tras la terminación o cambios de rol

SECCIÓN 4: GESTIÓN DE LA VULNERABILIDAD

- Se aplican parches de seguridad con prontitud para abordar las vulnerabilidades
- Existe un proceso para el escaneo de vulnerabilidades y las pruebas de penetración
- Se revisan y priorizan los parches de seguridad críticos en función del riesgo

SECCIÓN 5: POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

- Están documentadas y difundidas políticas y procedimientos de seguridad integrales
- Existe un programa de formación en materia de seguridad para los empleados
- Se revisan y actualizan las políticas de seguridad según sea necesario

SECCIÓN 6: MONITOREO Y REGISTRO

- Se revisan y monitorean periódicamente los eventos y registros de seguridad
- Existe un proceso para realizar alertas en tiempo real sobre actividades sospechosas
- Se han establecido procedimientos de respuesta a incidentes y de presentación de informes

SECCIÓN 7: RESPUESTA AL INCIDENTE

- Existe un plan de respuesta a incidentes que describa los pasos para abordar los incidentes de seguridad
- Están los empleados capacitados sobre cómo reconocer y reportar incidentes de seguridad
- Existe un proceso documentado para el análisis y la mejora posteriores al incidente

SECCIÓN 8: SEGURIDAD FÍSICA

- Existen controles de acceso físico para evitar el acceso no autorizado a los datos del titular de la tarjeta
- El acceso a áreas seguras está restringido y monitoreado
- Se mantienen videovigilancia y registros de visitantes para áreas sensibles

SECCIÓN 9: PROVEEDORES DE SERVICIOS DE TERCEROS

- Se evalúa el cumplimiento de PCI DSS de los proveedores externos
- Existen acuerdos escritos con proveedores de servicios para garantizar la protección de los datos del titular de la tarjeta
- Existe un proceso para monitorear y evaluar las prácticas de seguridad de terceros

Tenga en cuenta que esta lista de verificación proporciona una descripción general de alto nivel y es esencial realizar una análisis exhaustivo específico de los procesos y el contexto de su organización. Además, es Se recomienda colaborar con expertos o consultores de PCI DSS para realizar un análisis integral. Análisis de brechas para su organización.