TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MARCOS NORMATIVOS)

Unidad I – Trabajo práctico N°2

Profesor: Lic. Juan Pablo Villalba

Alumno: Balbuena Atar Dante Gabriel

Tucumán, Tafí Viejo – septiembre 2024

Tabla de contenido

1. Introducción 3

2. Desarrollo del requisito 9 3

3. Importancia de restringir el acceso físico 3

3.1 Controles de Acceso Físico 3

3.2 Monitoreo de Acceso 3

3.3 Destrucción de Datos Confidenciales 3

4. conclusiones 4

5. referencias 4

1. Introducción

Elegí el requisito 9 del estándar PCI-DSS ya que indica la necesidad de restringir el acceso físico a los datos de los titulares de tarjetas. Entre todos los aspectos importantes para la protección de estos datos sensibles se debe mencionar y aplicar a la seguridad física que se encarga de proteger los procesamientos, almacenamiento o transmisión en los sistemas de pago, teniendo en cuenta este punto importante que es la restricción del acceso físico a los datos de los titulares de tarjetas voy a mostrar el cuerpo o desarrollo a continuación para entender mejor este requisito.

2. Desarrollo del requisito 9

El Requisito 9 del estándar PCI DSS se centra en la protección física de los datos de los titulares de tarjetas, garantizando que solo el personal autorizado tenga acceso a los entornos donde se almacenan o procesan estos datos. Para lograrlo, se deben implementar controles físicos como sistemas de identificación, cerraduras, y dispositivos de monitoreo que aseguren la seguridad de los sistemas y eviten accesos no autorizados.
Entre las principales acciones recomendadas está la verificación de todos los visitantes, la supervisión de su acceso mediante acompañamiento por parte de empleados, y el mantenimiento de un registro detallado de sus entradas y salidas. También es crucial aplicar políticas rigurosas para la eliminación segura de medios o dispositivos que contengan datos sensibles una vez que ya no sean necesarios, asegurando que no puedan ser recuperados o reutilizados de manera no autorizada.
Estas medidas ayudan a prevenir amenazas tanto internas como externas, y son clave para cumplir con los lineamientos de seguridad del PCI DSS, protegiendo la integridad de los datos de los titulares de tarjetas frente a accesos físicos no permitidos

3. Importancia de restringir el acceso físico

En el mundo de la seguridad de datos, restringir el acceso físico a la información de los titulares de tarjetas es una medida fundamental para proteger la confidencialidad y la integridad de la información. La protección física juega un papel crucial dentro de los estándares PCI-DSS (Payment Card Industry Data Security Standard), que establecen estrictas directrices para salvaguardar los datos y prevenir posibles brechas de seguridad.

3.1 Controles de Acceso Físico

Los controles de acceso físico son esenciales para asegurar que solo las personas con autorización adecuada puedan ingresar a las áreas donde se almacenan o procesan datos sensibles. Estos controles pueden incluir una variedad de tecnologías y métodos, como el uso de tarjetas magnéticas, lectores biométricos (como huellas dactilares o reconocimiento facial), y cerraduras electrónicas. Implementar estos controles es vital para reducir el riesgo de accesos no autorizados y para proteger la información valiosa contra posibles amenazas.

3.2 Monitoreo de Acceso

El monitoreo constante del acceso físico es una medida crucial para detectar cualquier actividad sospechosa o potencialmente peligrosa. Esto se logra mediante la instalación de cámaras de videovigilancia, sistemas de alarmas, y la creación de registros detallados de acceso. Estos sistemas permiten una vigilancia continua y ayudan a identificar patrones inusuales que podrían indicar un intento de acceso no autorizado. La capacidad de reaccionar rápidamente ante cualquier anomalía es clave para mantener la seguridad.

3.3 Destrucción de Datos Confidenciales

La destrucción adecuada de datos confidenciales es una parte esencial de la protección de la información de los titulares de tarjetas. Cuando los datos ya no son necesarios, deben ser eliminados de manera que sea imposible recuperarlos. Esto incluye métodos como la desmagnetización de dispositivos de almacenamiento, la trituración física de medios y la sobreescritura de datos para asegurar que la información no pueda ser recuperada por personas no autorizadas. Estos métodos garantizan que la información sensible esté segura incluso después de su eliminación.

4. Conclusiones

En el requisito que seleccione (Restringir el acceso físico a los datos de los titulares de tarjetas) pude darme cuenta de la importancia de implementar esta medida ya que logra
Proteger físicamente los datos de los titulares de tarjetas que es crucial no solo para cumplir con las normativas, sino para construir una cultura de seguridad genuina. Cuando las organizaciones implementan controles de acceso físico efectivos, como sistemas de tarjetas y biometría, están creando un entorno en el que solo el personal autorizado puede acceder a áreas sensibles, lo que reduce significativamente el riesgo de brechas de seguridad. El monitoreo constante con cámaras y alarmas sirve como un sistema de alerta temprana, permitiendo identificar rápidamente cualquier actividad inusual y actuar antes de que se convierta en un problema mayor. Además, al asegurar una destrucción adecuada de datos mediante la trituración de dispositivos y técnicas de sobrescritura, se garantiza que la información confidencial no pueda ser recuperada ni utilizada indebidamente. Estas medidas, más allá de ser un cumplimiento normativo, reflejan un verdadero compromiso con la protección de la información y la confianza de los clientes. Invertir en estas prácticas demuestra que una empresa no solo se preocupa por cumplir con las reglas, sino por proteger realmente la privacidad y la seguridad de aquellos que confían en ella.

5. referencias

PCI-DSS Guide. (s.f.). Recuperado el 5 de septiembre de 2024, de https://pcidssguide.com/ Wikipedia. (2023, 27 de agosto). *Convenio sobre cibercriminalidad*.
https://es.wikipedia.org/wiki/Convenio_sobre_cibercriminalidad
RSI Security. (s.f.). Recuperado el 5 de septiembre de 2024, de https://blog.rsisecurity.com/
Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).