IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

Agenda

- **Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta**
- **Requisito 11: Probar periódicamente los sistemas y procesos de seguridad**
- **Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal**

Objetivos esperados

El alumno será capaz de:

- Conocer y ser capaz de implementar los tres siguientes requisitos de la norma PCI DSS:
  - Rastrear y supervisar todos los accesos a los recursos de red y a los datos del titular de la tarjeta.
  - Probar periódicamente los sistemas y procesos de seguridad.
  - Mantener una política que aborde la seguridad de la información para todo el personal.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

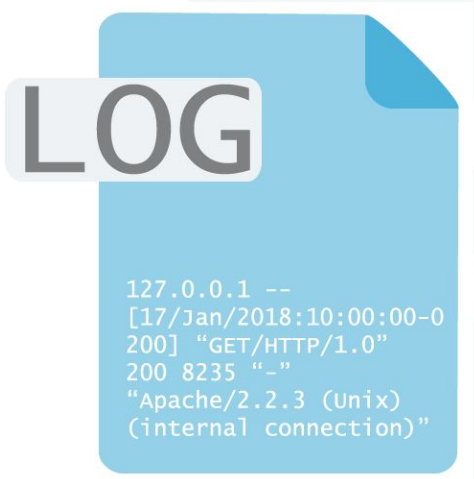
ALIGNMENT

Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta

Requisito 10

Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta

Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el **rastreo, la alerta y el análisis** cuando algo no funciona bien. Determinar la causa de un riesgo es muy difícil, sino imposible, sin los registros de la actividad del sistema.



Requisito 10

10.1 Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos.

10.2 Implemente pistas de auditoría automáticas en todos los componentes del sistema a fin de reconstruir los siguientes eventos:

- Todo acceso por parte de usuarios a los datos del titular de la tarjeta.
- Todas las acciones realizadas por personas con privilegios de raíz o administrativos
- Acceso a todas las pistas de auditoría
- Intentos de acceso lógico no válidos
- Uso y cambios de los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y el aumento de privilegios, y de todos los cambios, incorporaciones y eliminaciones de las cuentas con privilegios administrativos o de raíz.
- Inicialización, detención o pausa de los registros de auditoría
- Creación y eliminación de objetos en el nivel del sistema

Requisito 10

10.3 Registre, al menos, las siguientes entradas de pistas de auditoría de los componentes del sistema para cada evento:

- Identificación de usuarios
- Tipo de evento
- Fecha y hora
- Indicación de éxito o fallo
- Origen del evento
- Identidad o nombre de los datos, componentes del sistema o recursos afectados.

10.4 Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos.

10.5 Proteja las pistas de auditoría para que no se puedan modificar.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 10

10.6 Revise los registros y los eventos de seguridad en todos los componentes del sistema para identificar anomalías o actividades sospechosas.

10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses.

10.8 Requisitos adicionales solo para los proveedores de servicios: Implementar un proceso para la detección y el informe oportunos de fallas de los sistemas de control de seguridad crítica, lo que incluye, sin carácter restrictivo, la falla de lo siguiente:

- Firewalls - IDS/IPS - FIM - Antivirus - Controles de acceso físicos - Controles de acceso lógico - Mecanismos de registro de auditoría - Controles de segmentación (si se utilizan)

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 10

10.9 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear todos los accesos a los recursos de la red y a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

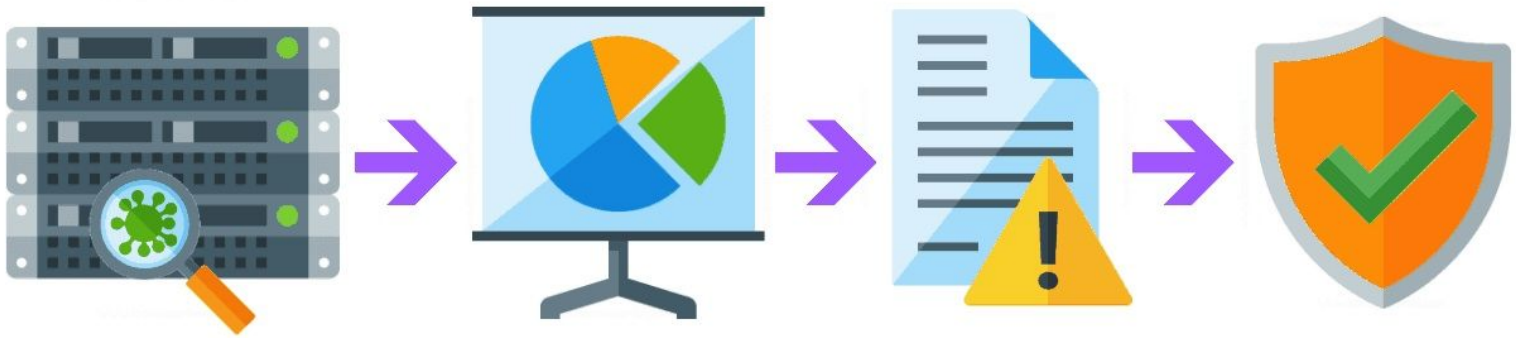
ALIGNMENT

Requisito 11: Probar periódicamente los sistemas y procesos de seguridad

Requisito 11

Pruebe con regularidad los sistemas y procesos de seguridad.

Las **vulnerabilidades** son descubiertas continuamente por personas malintencionadas e investigadores y son introducidas mediante software nuevo. Los componentes del sistema, los procesos y el software personalizado deben evaluarse con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico.



Requisito 11

11.1 Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11), detecte e identifique, trimestralmente, todos los puntos de acceso inalámbricos autorizados y no autorizados:

- Lleve un inventario de los puntos de acceso inalámbricos autorizados que incluyan una justificación comercial documentada.
- Implemente procedimientos de respuesta a incidentes en caso de que se detecten puntos de acceso inalámbricos no autorizados.

Requisito 11

11.2 Realice análisis internos y externos de las vulnerabilidades de la red, al menos, trimestralmente y después de cada cambio significativo en la red (como por ejemplo, la instalación de nuevos componentes del sistema, cambios en la topología de la red, modificaciones en las normas de firewall, actualizaciones de productos).

- **Internos**: Aborde las vulnerabilidades y realice redigitalizaciones para verificar que todas las vulnerabilidades de "alto riesgo" se resuelven de acuerdo con la clasificación de la vulnerabilidad de la entidad (según el Requisito 6.1). Los análisis deben estar a cargo de personal calificado.
- **Externos**: Los análisis trimestrales de vulnerabilidades externas deben estar a cargo de un ASV (proveedor aprobado de escaneo) que esté certificado por el PCI SSC (PCI Security Standards Council). Vuelva a realizar los análisis cuantas veces sea necesario hasta que todos los análisis estén aprobados.
- Lleve a cabo análisis internos y externos, y repítalos, según sea necesario, después de realizar un cambio significativo. Los análisis deben estar a cargo de personal calificado.

Requisito 11

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Escala CVSS v2.0 y v3.0

Categorías de CVSS v2.0

Categorías de CVSS v3.0

Requisito 11

11.3 Desarrolle e implemente una metodología para las pruebas de penetración internas y externas, al menos una vez al año y después de un cambio significativo, que incluya lo siguiente:

- Esté basada en los enfoques de pruebas de penetración aceptados por la industria (por ejemplo, NIST SP800- 115).
- Incluya cobertura de todo el perímetro del CDE (entorno de datos del titular de la tarjeta) y de los sistemas críticos.
- Incluya pruebas del entorno interno y externo de la red.
- Incluya pruebas para validar cualquier segmentación y controles de reducción del alcance.
- Defina las pruebas de penetración de la capa de la aplicación para que incluyan, al menos, las vulnerabilidades enumeradas en el Requisito 6.5.
- Defina las pruebas de penetración de la capa de la red para que incluyan los componentes que admiten las funciones de red y los sistemas operativos
- Incluya la revisión y evaluación de las amenazas y vulnerabilidades ocurridas en los últimos 12 meses.
- Especifique la retención de los resultados de las pruebas de penetración y los resultados de las actividades de corrección.

Requisito 11

11.4 Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red.

- Supervise todo el tráfico presente en el perímetro y en los puntos críticos del entorno de datos de titulares de tarjetas y alertar al personal ante la sospecha de riesgos.
- Mantenga actualizados todos los motores, bases y firmas de detección y prevención de intrusiones.

11.5 Implemente un mecanismo de detección de cambios (por ejemplo, herramientas de supervisión de integridad de archivos) para alertar al personal sobre modificaciones (incluyendo cambios, adiciones y eliminaciones) no autorizadas de archivos críticos del sistema, de archivos de configuración o de contenido, y configure el software para realizar comparaciones de archivos críticos, al menos, una vez por semana.

Requisito 11

11.6 Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

Coffee Break

20 min.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 12: Mantener una política que aborde la seguridad de la información para todo el personal

Requisito 12

Mantenga una política que aborde la seguridad de la información para todo el personal.

Una política de seguridad sólida establece el grado de seguridad para toda la entidad e informa al personal lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de sus responsabilidades para protegerlos. A los fines del Requisito 12, el término "**personal**" hace referencia a los empleados de tiempo completo y parcial, a los empleados temporales, a los contratistas y consultores que "residen" en las instalaciones de la entidad o que tienen acceso al entorno de datos del titular de la tarjeta.

Requisito 12

12.1 Establezca, publique, mantenga y distribuya una política de seguridad.

- Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno.

12.2 Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente:

- Se realiza, al menos, una vez al año y después de implementar cambios significativos en el entorno
- Identifica activos críticos, amenazas y vulnerabilidades
- Los resultados en un análisis formal y documentado de riesgo.

Requisito 12

12.3 Desarrolle políticas de uso de tecnologías críticas para definir su uso adecuado por todo el personal.

- Estos incluyen acceso remoto, inalámbrico, medios electrónicos extraíbles, computadoras portátiles, tabletas, dispositivos portátiles, correo electrónico e Internet.

12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal.

Requisito 12

12.5 Asigne a una persona o a un equipo las siguientes responsabilidades de administración de seguridad de la información:

- Establezca, documente y distribuya las políticas y los procedimientos de seguridad.
- Monitoree y analice las alertas y la información de seguridad y comuníquelas al personal correspondiente.
- Establezca, documente y distribuya los procedimientos de escalamiento y respuesta ante incidentes de seguridad para garantizar un manejo oportuno y efectivo de todas las situaciones.
- Administre las cuentas de usuario, incluso las incorporaciones, eliminaciones y modificaciones.
- Monitoree y controle todo acceso a los datos.

12.6 Implemente un programa formal de concienciación sobre seguridad para que todo el personal tome conciencia de la importancia de la seguridad de los datos del titular de la tarjeta.

Requisito 12

12.7 Examine al personal potencial antes de contratarlo a fin de minimizar el riesgo de ataques desde fuentes internas. (Entre los ejemplos de verificaciones de antecedentes se incluyen el historial de empleo, registro de antecedentes penales, historial crediticio y verificación de referencias).

12.8 Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos del titular de la tarjeta, o que podrían afectar la seguridad de los datos del titular de la tarjeta.

12.9 Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta que ellos poseen, almacenan, procesan o transmiten en nombre del cliente, o en la medida en que puedan afectar la seguridad del entorno de datos del titular de la tarjeta del cliente.

Requisito 12

12.10 Implemente un plan de respuesta ante incidentes. Estar preparado para responder de inmediato ante una violación del sistema.

12.11 Requisitos adicionales solo para los proveedores de servicios: Realizar revisiones al menos cada tres meses para confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos. Las revisiones deben abarcar los siguientes procesos:

- Revisiones del registro diario
- Revisiones del conjunto de reglas de firewall
- La aplicación de las normas de configuración a los nuevos sistemas
- Respuesta a las alertas de seguridad
- Procesos de gestión del cambio

12.11.1 Requisitos adicionales solo para los proveedores de servicios: Mantener la documentación del proceso de revisión trimestral

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

CONSULTAS

Profesoras del Curso

Ingeniera en Información y Control de Gestión de la Universidad de Chile, Diplomada en Seguridad de la Información y Ciberseguridad de la Universidad de Santiago de Chile. Especialista en norma PCI DSS, con certificación internacional Internal Security Assessor ISA-PCI. Posee las certificaciones de:

- Internal Security Assessor (ISA-PCI)
- Implementador de SGSI bajo ISO 27.001
- Gobierno y Gestión de la Ciberseguridad
- Herramientas de Ciberseguridad
- Introducción a la Criptografía

vaniavillavicenciomaza

vavillavice@gmail.com

Contador Auditor de la Universidad de Chile, Diplomada en Seguridad de la Información y Ciberseguridad de la Universidad de Santiago de Chile. Especialista en norma PCI DSS. Posee las certificaciones de:

- Implementador de SGSI bajo ISO 27.001
- Gobierno y Gestión de la Ciberseguridad
- Herramientas de Ciberseguridad
- Introducción a la criptografía

paulacelisquiroz

paulacelisquiroz@gmail.com

IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza