IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Agenda

- **Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa**
- **Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora**
- **Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta**

Objetivos esperados

El alumno será capaz de:

- Conocer y ser capaz de implementar los tres siguientes requisitos de la norma PCI DSS:
  - Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
  - Asignar una ID exclusiva a cada persona que tenga acceso por computadora.
  - Restringir el acceso físico a los datos del titular de la tarjeta.

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa

Requisito 7

Desarrollar y mantener sistemas y aplicaciones seguros.

A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que **limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo**.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 7

7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.

7.2 Establezca un sistema de control de acceso para los componentes del sistema que restrinja el acceso según la necesidad del usuario de saber, y esté configurado para "denegar todo" a menos que se permita específicamente.

7.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso 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 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora

Requisito 8

Asignar una ID exclusiva a cada persona que tenga acceso por computadora.

Al asignar una **ID exclusiva** a cada persona que tenga acceso garantiza que cada una se hará responsable de sus actos. Cuando se ejerce dicha responsabilidad, las medidas implementadas en datos y sistemas críticos están a cargo de procesos y usuarios conocidos y autorizados y, además, se puede realizar un seguimiento. La eficacia de una contraseña se determina, en gran medida, por el diseño y la implementación del sistema de autenticación, especialmente, la frecuencia con la que el atacante intenta obtener la contraseña y los métodos de seguridad para proteger las contraseñas de usuarios en los puntos de acceso durante la transmisión y el almacenamiento.

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

Requisito 8

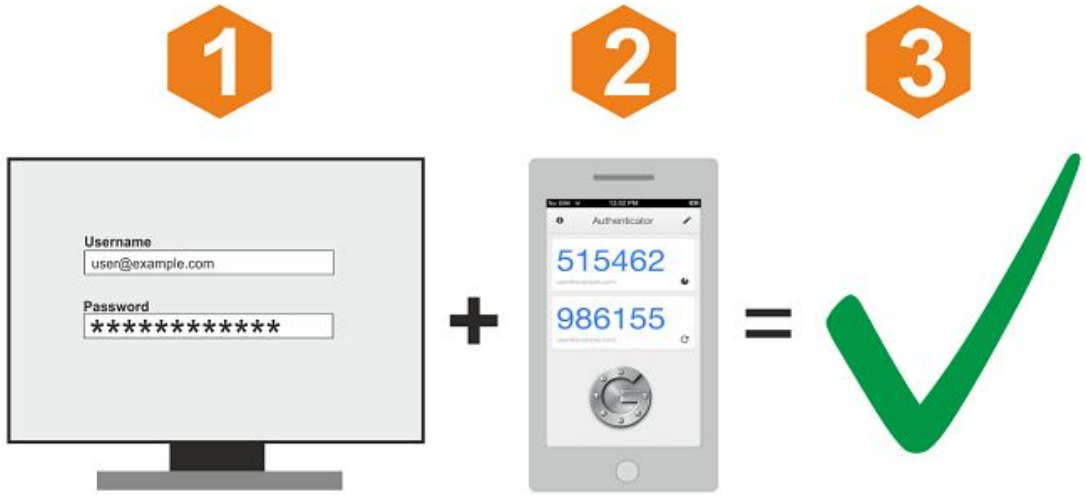
8.1 Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema.

- Asigne a todos los usuarios una **ID exclusiva** antes de permitirles acceder a los componentes del sistema o a los datos del titular de la tarjeta.
- **Cancele** de inmediato el **acceso** a cualquier usuario **cesante**.
- **Administre las ID que usan los terceros** para acceder, respaldar o mantener los componentes del sistema.

Requisito 8

8.2 Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios para usuarios no consumidores y administradores en todos los componentes del sistema y que se use, al menos, uno de los siguientes métodos para autenticar todos los usuarios:

- Algo que el usuario sepa, como una contraseña o frase de seguridad.
- Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente.
- Algo que el usuario sea, como un rasgo biométrico.



Requisito 8

8.3 Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores (MFA).

8.4 Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios.

8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas, ni otros métodos de autenticación:

Requisitos adicionales solo para los proveedores de servicios: Los proveedores de servicios que tengan acceso a las instalaciones del cliente (por ejemplo, para tareas de soporte de los sistemas de POS o de los servidores) deben usar una credencial de autenticación exclusiva (como una contraseña/frase) para cada cliente.

Requisito 8

8.6 El uso de otros mecanismos de autenticación, como tokens de seguridad física, tarjetas inteligentes y certificados, debe asignarse a una cuenta individual.

8.7 Todo acceso a cualquier base de datos que contenga datos de titulares de tarjetas debe estar restringido:

- Todo acceso de usuarios debe ser a través de métodos programáticos.
- Sólo los administradores de bases de datos pueden tener acceso directo o de consulta.
- Solo las aplicaciones pueden usar las ID de aplicaciones para las aplicaciones de base de datos.

8.8 Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

Coffee Break

20 min.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta

Requisito 9

Restringir el acceso físico a los datos del titular de la tarjeta.

Cualquier **acceso físico** a datos o sistemas que alojen datos de titulares de tarjetas permite el acceso a dispositivos y datos, así como también permite la eliminación de sistemas o copias en papel, y se debe restringir correctamente.

A los fines del Requisito 9, "**empleados**" se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que estén físicamente presentes en las instalaciones de la entidad. "**Visitante**" se define como proveedor, invitado de algún empleado, personal de servicio o cualquier persona que necesite ingresar a las instalaciones durante un tiempo no prolongado, generalmente no más de un día. "**Medios**" hace referencia a todos los medios en papel y electrónicos que contienen datos del titular de la tarjeta.

Requisito 9

9.1 Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.

9.2 Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes.

9.3 Controle el acceso físico de los empleados a las áreas confidenciales:

- El acceso debe estar autorizado y basarse en la función de cada persona.
- El acceso debe cancelarse inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, deben devolverse o desactivarse.

9.4 Implemente procedimientos para identificar y autorizar a los visitantes.

Requisito 9

9.5 Proteja físicamente todos los medios.

9.6 Lleve un control estricto de la distribución interna o externa de todos los tipos de medios.

9.7 Lleve un control estricto del almacenamiento y la accesibilidad de los medios.

9.8 Destruya los medios cuando ya no sea necesario guardarlos por motivos comerciales o legales.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 9

9.9 Proteja los dispositivos que capturan datos de tarjetas de pago mediante la interacción física directa con la tarjeta para proporcionar protección contra alteraciones y sustituciones.

9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico 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

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