DIPLOMADO
CIBERSEGURIDAD

IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

Agenda

- Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta
- Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad
- Requisito 3: Proteger los datos almacenados del titular de la tarjeta

Objetivos esperados

El alumno será capaz de:

- Conocer y ser capaz de implementar los tres primeros requisitos de la norma PCI DSS:
  - Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.
  - No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
  - Proteger los datos almacenados del titular de la tarjeta.

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta

IMPLEMENTADOR PCI/DSS

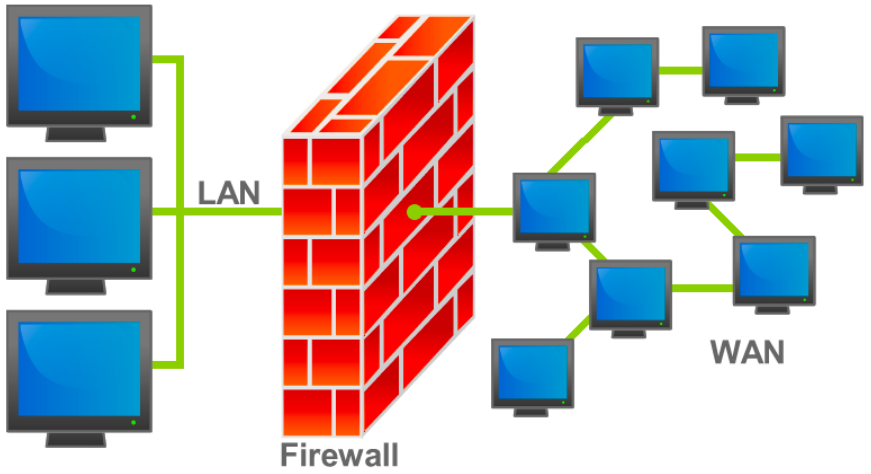
DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 1

Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.

Los firewalls son dispositivos que controlan el tráfico computarizado entre las redes (internas) y las redes no confiables (externas) de una entidad, así como el tráfico de entrada y salida a áreas más sensibles dentro de las redes internas confidenciales de una entidad.



IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 1

¿Trabajan con algún firewall dentro de su organización?

¿Cuál?

¿Cuáles conocen?

Requisito 1

1.1 Normas de configuración para firewalls y routers:

- Tener un diagrama de red actualizado que muestre todos los flujos de datos de tarjetahabiente.
- Instalar un firewall entre Internet, DMZ y red interna.
- Configurar de puertos, servicios y protocolos seguros, con su respectiva documentación y justificación de negocio.
- Revisar normas de configuración cada 6 meses.

1.2 Restringir las conexiones entre redes no confiables y cualquier componente del sistema en el CDE:

- Restringir el tráfico entrante y saliente al CDE.
- Sincronizar archivos de configuración de routers.
- Instalar firewall entre wireless y CDE.

Requisito 1

1.3 Prohibir el acceso público directo entre Internet y cualquier componente del CDE.

1.4 Instalar un software de firewall personal o una funcionalidad equivalente en cualquier dispositivo que se conecta a Internet cuando está fuera de la red y que también se usan para acceder al CDE:

- Definir ajustes específicos
- Tener activa la función del firewall personal
- El firewall personal no debe ser alterable por los usuarios.

1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, en uso y conocidos por todas las partes afectadas.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 2: No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad

Requisito 2

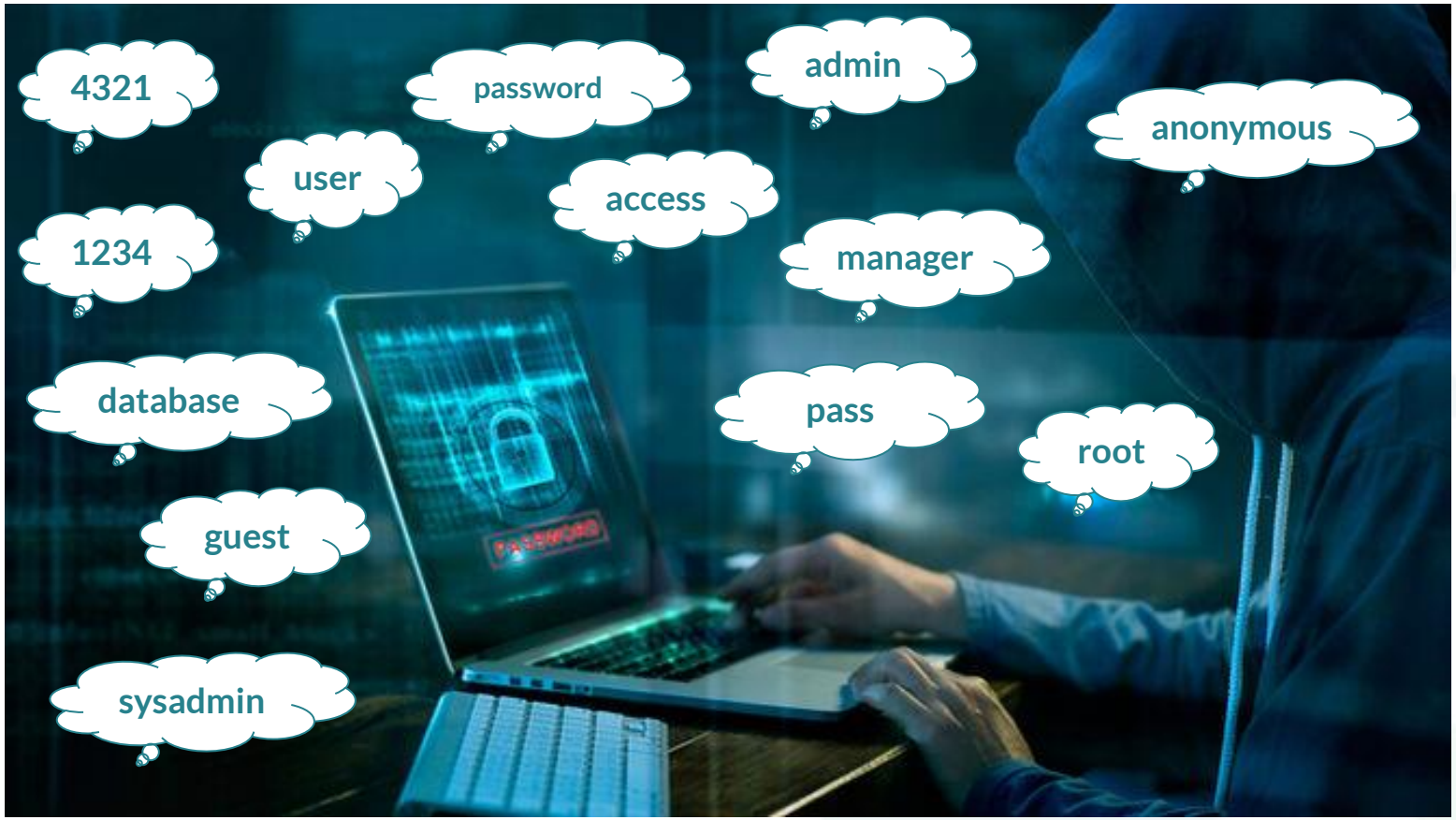
No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

Las personas malintencionadas (externas e internas a una entidad), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para comprometer los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se determinan fácilmente por medio de información pública.

Requisito 2

2.1 Siempre cambie los valores predeterminados por el proveedor y elimine/deshabilite las cuentas predeterminadas innecesarias antes de instalar un sistema en la red:

- No utilizar contraseñas que vienen por defecto



Requisito 2

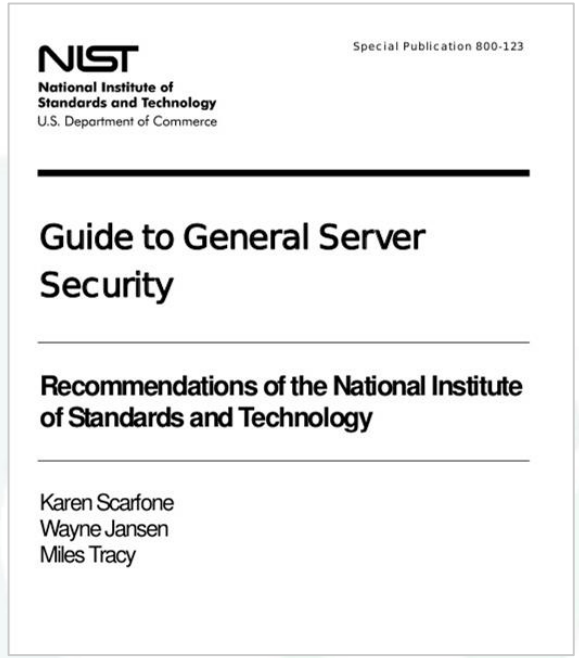
2.2 Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria (CIS, ISO, SANS, NIST):

- Implementar sólo una función principal por servidor.
- Eliminar todas las funcionalidades innecesarias

SANS

CIS Center for Internet Security®

ISO


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-123

Guide to General Server Security

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Wayne Jansen
Miles Tracy

Requisito 2

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

¿Ha participado en algún proceso de hardening dentro de su organización?

¿Ha utilizado alguna norma o checklist de referencia?

¿Cuál?

Requisito 2

2.3 Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido.

2.4 Lleve un inventario de los componentes del sistema que están dentro del alcance PCI DSS.

2.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los parámetros predeterminados del proveedor y otros parámetros de seguridad estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 2

2.6 Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad. Estos proveedores deben cumplir requisitos específicos detallados en el Anexo A1: Requisitos adicionales de las DSS de la PCI para los proveedores de servicios de hosting.

Requisito 2

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

¿Cuáles componentes de sistema creen que debemos incluir en el inventario?

Coffee Break

20 min.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 3: Proteger los datos almacenados del titular de la tarjeta

Requisito 3

Proteger los datos almacenados del titular de la tarjeta.

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas.

Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos.

También se deberían considerar otros métodos eficaces para proteger los datos almacenados para mitigar posibles riesgos.

Por ejemplo, los métodos para minimizar el riesgo incluyen:

- **No almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario**;
- Truncar los datos del titular de la tarjeta si no se necesita el PAN completo y;
- No enviar el PAN utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT

Requisito 3

3.1 Limite el almacenamiento de datos y el tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio.

- Implementar políticas, procedimientos y procesos de retención y eliminación de datos.
- Implementar un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida

Requisito 3

3.2 No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos confidenciales de autenticación, convertir todos los datos en irrecuperables al finalizar el proceso de autorización.

- Los emisores y las entidades relacionadas pueden almacenar datos confidenciales de autenticación si existe una justificación comercial y los datos se almacenan de forma segura.

Requisito 3

3.3 Enmascare el PAN (número de cuenta principal) cuando aparezca (los primeros seis o los últimos cuatro dígitos es la cantidad máxima de dígitos que aparecerá), de modo que solo el personal con una necesidad comercial legítima pueda ver más que los primeros seis o los últimos cuatro dígitos del PAN.

- Esto no reemplaza los requisitos más estrictos que pueden existir para la visualización de los datos del titular de la tarjeta, como en un recibo del punto de venta (POS).

3.4 Convierta el PAN en ilegible en cualquier lugar donde se almacene (incluídos los datos que se almacenen en medios digitales portátiles, en medios de copia de seguridad y en registros).

- Utilizar cualquiera de los siguientes métodos: Valores hash de una vía basados en criptografía sólida; Truncamiento; Tokens y ensambladores de índices; Criptografía sólida con procesos y procedimientos asociados para la administración de claves.

Requisito 3

3.5 Documente e implemente procedimientos que protejan las claves utilizadas para proteger los datos del titular de la tarjeta almacenados contra su posible divulgación o uso indebido.

3.6 Documente por completo e implemente todos los procesos y procedimientos de administración de claves de las claves criptográficas que se utilizan para el cifrado de CHD.

3.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados 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

vania.villavicencio@usach.cl

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

paula.celis.q@usach.cl

DIPLOMADO
CIBERSEGURIDAD

IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza