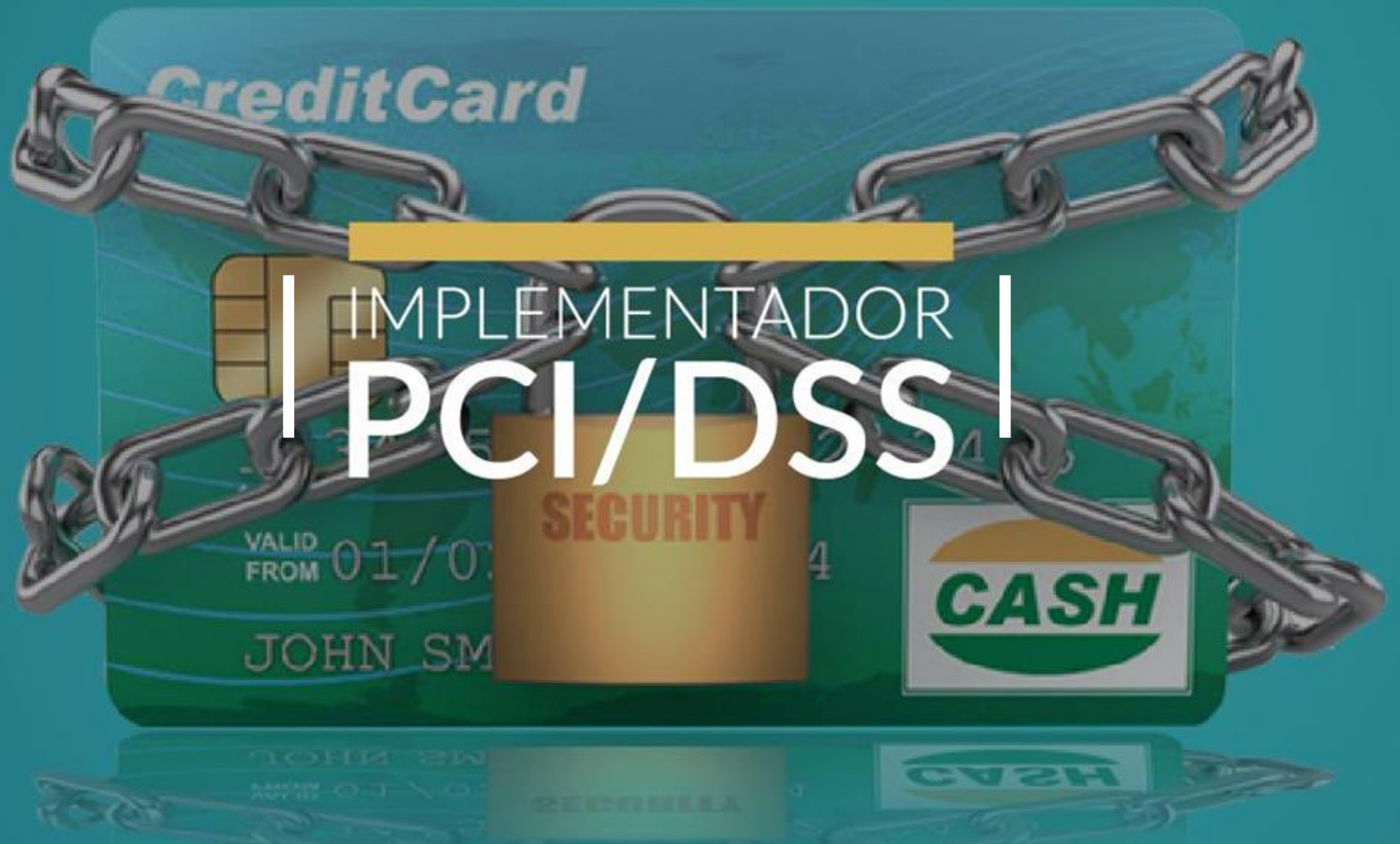
DIPLOMADO
CIBERSEGURIDAD



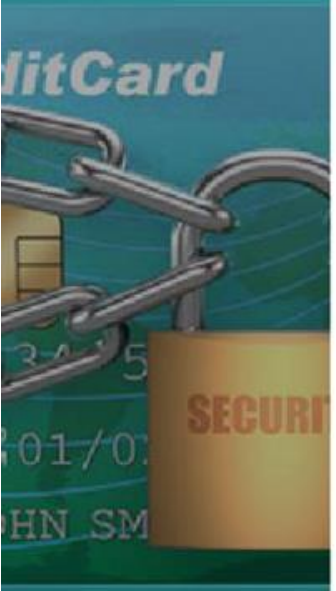
IMPLEMENTADOR PCI/DSS

Profesoras
Paula Celis Quiroz
Vania Villavicencio Maza

IMPLEMENTADOR PCI/DSS

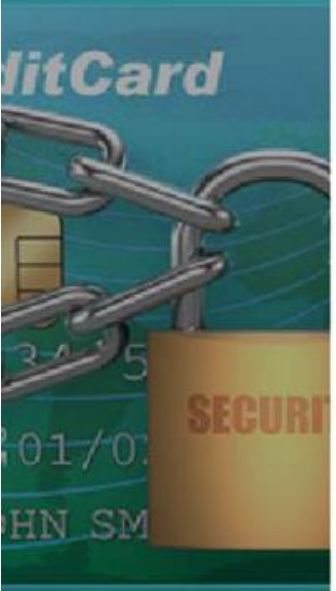
DIPLOMADO CIBERSEGURIDAD

ALIGNMENT



Agenda

- **Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas**
- **Requisito 5: Utilizar y actualizar con regularidad los programas o software antivirus**
- **Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros**



Objetivos esperados

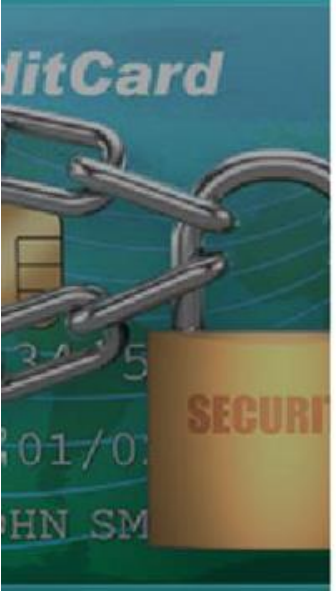
El alumno será capaz de:

- Conocer y ser capaz de implementar los siguientes 3 requisitos de la norma PCI DSS:
  - Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
  - Utilizar y actualizar con regularidad los programas o software antivirus.
  - Desarrollar y mantener sistemas y aplicaciones seguros.

IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT

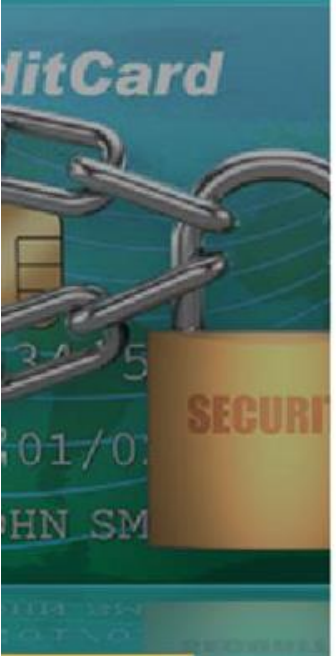


Requisito 4: Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas

Requisito 4

Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

La información confidencial se debe cifrar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación siguen siendo los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.



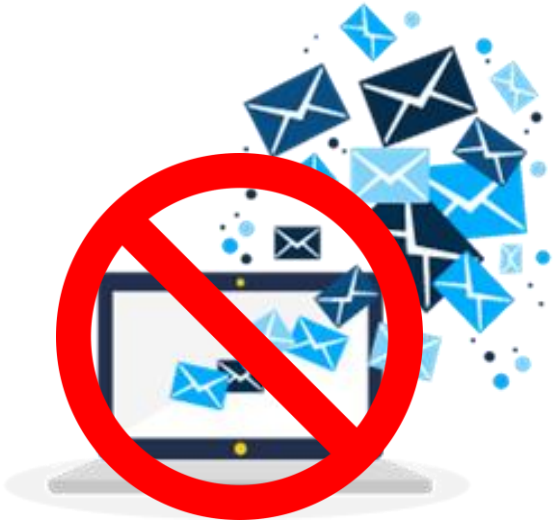
Requisito 4

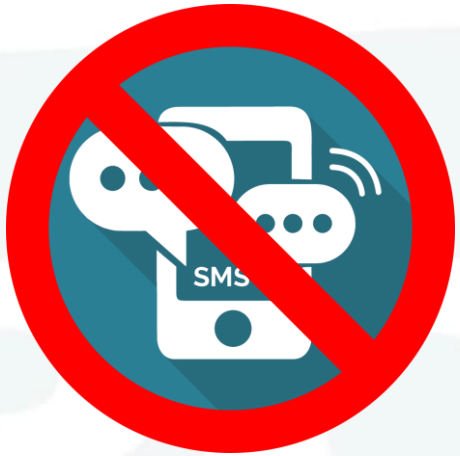
4.1 Utilice criptografía sólida y protocolos de seguridad para proteger los datos del titular de la tarjeta confidenciales durante la transmisión por redes públicas abiertas.

- Asegúrese de que las redes inalámbricas que transmiten datos del titular de la tarjeta o que estén conectadas al entorno de datos del titular de la tarjeta utilicen las mejores prácticas de la industria para implementar un cifrado sólido para la autenticación y transmisión.

Requisito 4

4.2 Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, SMS, el chat, etc.).

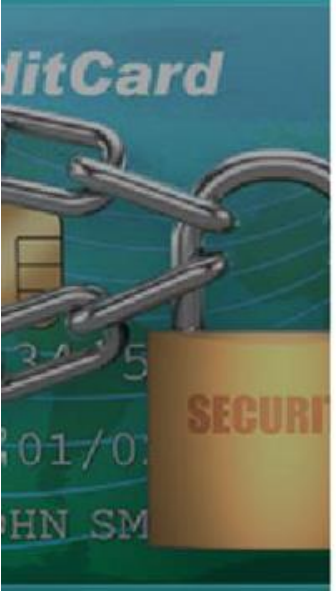




IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT



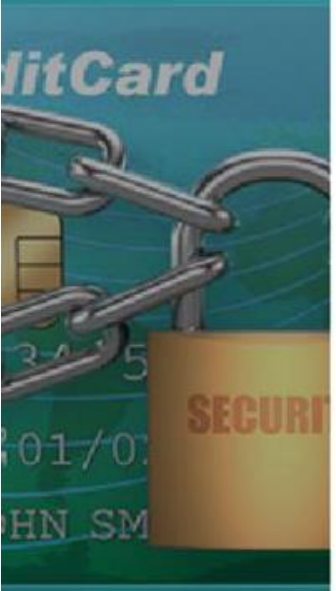
Requisito 4

4.3 Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas

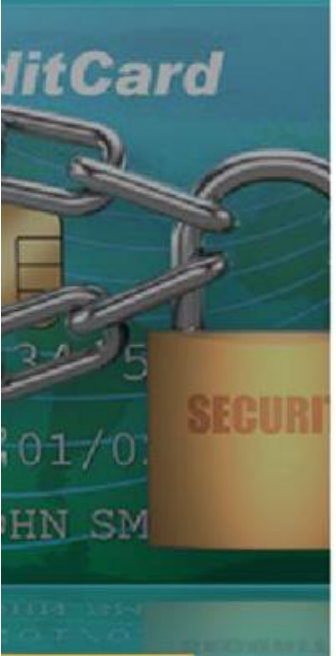
IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT



Requisito 5: Utilizar y actualizar con regularidad los programas o software antivirus



Requisito 5

Utilizar y actualizar con regularidad los programas o software antivirus.

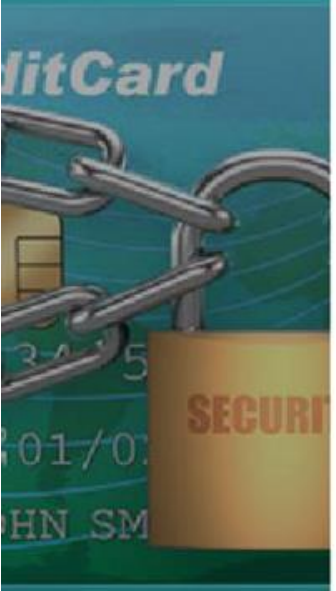
El software malicioso, llamado "malware", incluidos los virus, los gusanos (worm) y los troyanos (Trojan), ingresa a la red durante muchas actividades de negocio aprobadas incluidos los correos electrónicos de los trabajadores y la utilización de Internet, de computadoras portátiles y de dispositivos de almacenamiento y explota las vulnerabilidades del sistema.

El software antivirus deberá utilizarse en todos los sistemas que el malware, por lo general, afecta para proteger los sistemas contra las amenazas de software maliciosos actuales o que eventualmente se desarrollen. Se puede considerar la opción de incluir otras soluciones antimalware como complemento del software antivirus; no obstante, estas soluciones adicionales no reemplazan la implementación del software antivirus.

Requisito 5

5.1 Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadores personales y servidores).

- Para los sistemas que no son comúnmente afectados por software malicioso, realice evaluaciones periódicas para evaluar las amenazas de malware en evolución y confirme si dichos sistemas continúan sin requerir software antivirus.



Requisito 5

5.2 Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente:

- Estén actualizados.
- Ejecuten análisis periódicos.
- Generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de PCI DSS.

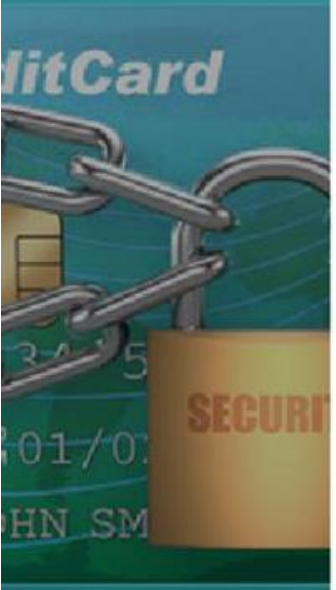
> **10.7 Conserve el historial de pistas de auditorías durante, al menos, un año, con un mínimo de disponibilidad para análisis de tres meses.**

5.3 Asegúrese de que los mecanismos de antivirus funcionen activamente y que los usuarios no puedan deshabilitarlos ni alterarlos, salvo que estén específicamente autorizados por la gerencia en casos particulares y durante un período limitado.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT



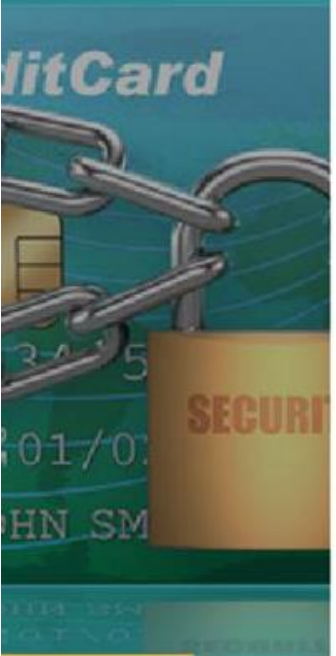
Requisito 5

5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

IMPLEMENTADOR PCI/DSS

DIPLOMADO CIBERSEGURIDAD

ALIGNMENT



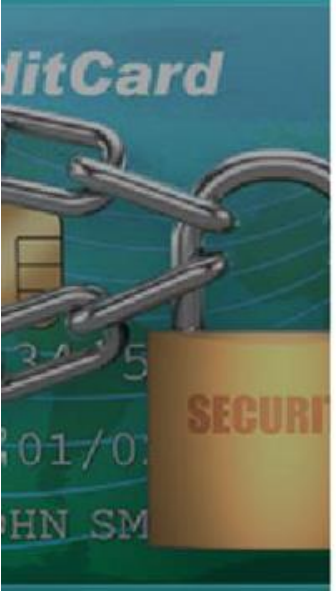
Coffee Break

20 min.

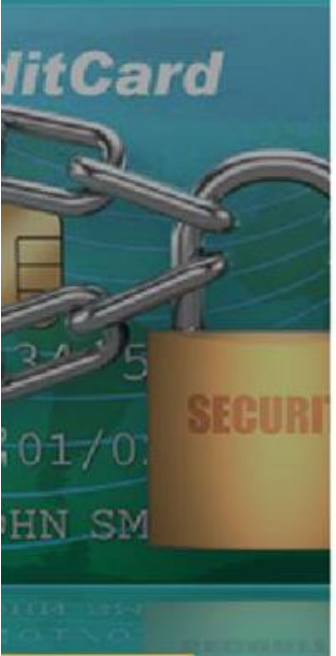
IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT



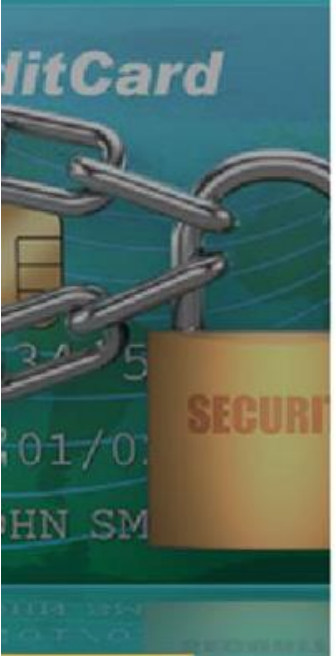
Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros



Requisito 6

Desarrollar y mantener sistemas y aplicaciones seguros.

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades pueden subsanarse mediante **parches de seguridad** proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas deben contar con los parches de software correctos para evitar que personas malintencionadas o software maliciosos usen, de manera indebida, o pongan en riesgo los datos del titular de la tarjeta.



Requisito 6

6.1 Establezca un proceso para identificar las vulnerabilidades de seguridad por medio de fuentes externas conocidas para obtener información sobre las vulnerabilidades de seguridad, y asigne una clasificación de riesgo (por ejemplo, “alto”, “medio” o “bajo”) a las vulnerabilidades de seguridad recientemente descubiertas.

- Por ejemplo, los criterios para clasificar vulnerabilidades pueden incluir la puntuación base del CVSS, la clasificación del proveedor o el tipo de sistema afectado.

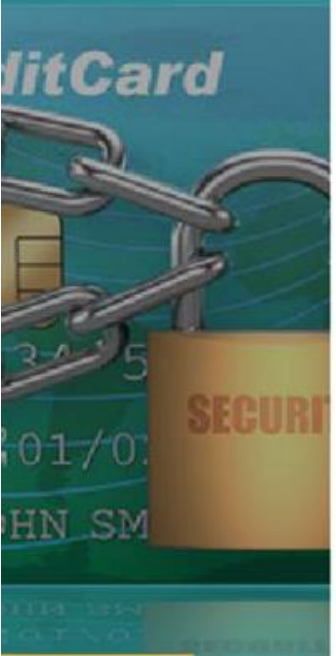
6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad proporcionados por los proveedores que ofrecen protección contra vulnerabilidades conocidas.

- Instalar los parches importantes de seguridad dentro de un plazo de un mes de su lanzamiento.
- Instalación de todos los parches de seguridad proporcionados por el proveedor en un período coherente (por ejemplo, en un período de tres meses).

Requisito 6

6.3 Desarrolle aplicaciones de software internas y externas (incluso acceso administrativo a aplicaciones basado en web) de acuerdo con PCI DSS y según las mejores prácticas de la industria.

- Incorpore seguridad de la información durante todo el ciclo de vida del desarrollo de software. Esto se aplica a todo el software desarrollado internamente, así como a la medida o software personalizado desarrollado por un tercero.



Requisito 6

6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. Asegúrese de que todos los requisitos relevantes de PCI DSS se implementen en sistemas y redes nuevos o modificados después de cambios significativos.

6.5 Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo de software:

- Capacite a los desarrolladores, por lo menos anualmente, en las técnicas actualizadas de codificación segura, incluida la forma de evitar las vulnerabilidades de codificación comunes.
- Desarrollar aplicaciones basadas en directrices de codificación seguras.

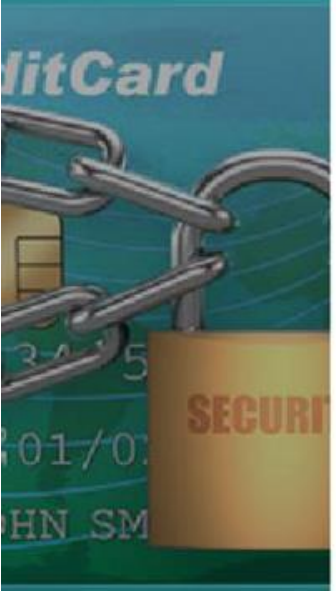
Requisito 6

6.6 En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente y asegúrese de que estas aplicaciones se protejan contra ataques conocidos con alguno de los siguientes métodos:

- Controlar las aplicaciones web públicas mediante herramientas o métodos de evaluación de seguridad de vulnerabilidad de aplicación automáticas o manuales, por lo menos, anualmente y después de cada cambio.
- Instalación de una solución técnica automática que detecte y prevenga ataques web (por ejemplo, firewall de aplicación web) delante de aplicaciones web públicas a fin de controlar el tráfico continuamente.

Requisito 6

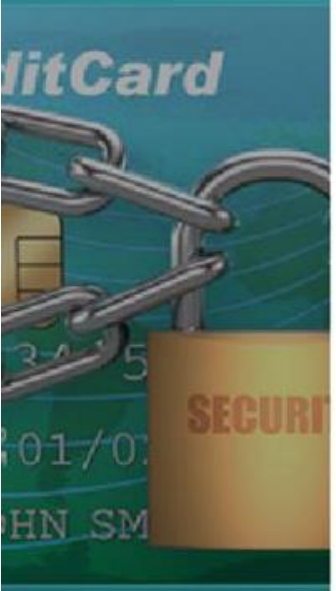
6.7Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.



IMPLEMENTADOR
PCI/DSS

DIPLOMADO
CIBERSEGURIDAD

ALIGNMENT



CONSULTAS

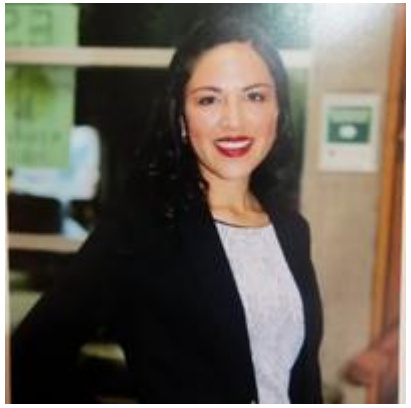
Profesoras del Curso

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



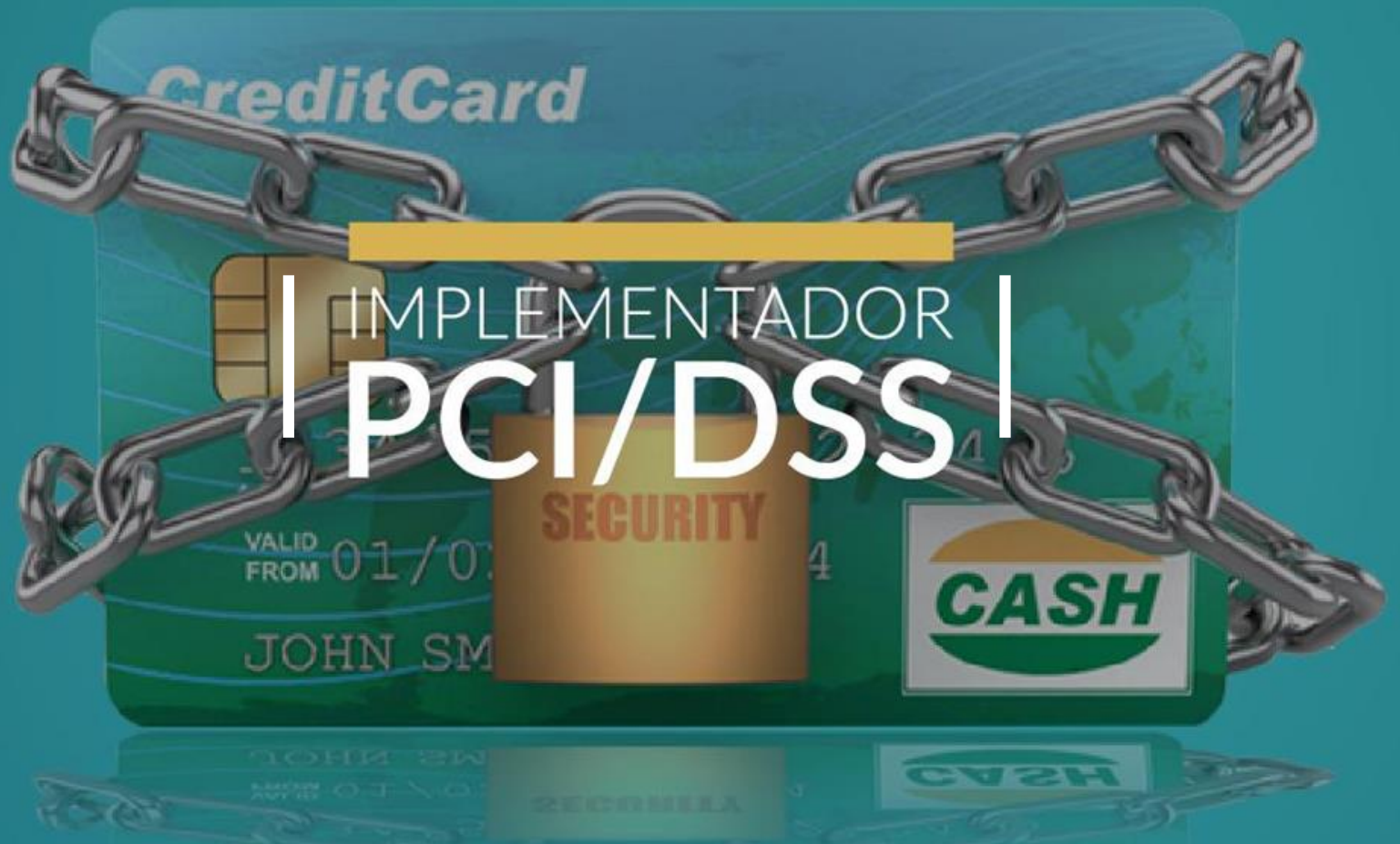
Contador Auditor de la Universidad de Chile, Diplomada en Seguridad de la Información y Ciberseguridad de la Universidad de Santiago de Chile. Especialista en norma PCI DSS. Posee las certificaciones de:

- 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