Ingeniería de Sistemas

PCI DSS

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

Robos de Tarjetas de pago (I)

- **9 de enero de 2000**:

  Robo de 25.000 números de tarjetas de crédito y direcciones en CDUniverse.com (comercio de música online) para ser puestos posteriormente a la venta en Internet.

- **22 de mayo de 2005**:

  Master Card informa de la existencia de 40 millones de tarjetas de crédito en riesgo

- **Julio de 2005 a enero de 2007**:

  La firma minorista TJX anuncia el robo de 46,5 millones de tarjetas de crédito por hackers desconocidos

Robos de Tarjetas de pago (I)

- **Caso Target**
  - http://cnnespanol.cnn.com/2014/01/10/70-millones-de-clientes-de-target-afectados-por-hackeo-de-informacion/
- **Caso Home Depot**
- https://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

UNIVERSIDAD DE LIMA

¿Cuánto vale la información robada? (I)

How much is your data worth?

Hacker service	Price
Visa or MasterCard credentials	**$7**
Credit card with magnetic stripe or chip data	**$15**
Premium American Express, Discover Card, MasterCard or Visa with strip or chip data	**$30**
Bank account credentials (balance of $15,000)	**$500**
Bank account credentials (balance of $70,000 to $150,000)	**6% of account balance**
Large U.S. airline points accounts	**1.5 million points cost $450**
Large international hotel chain points account	**1 million points cost $200**

SIDAD

- No es preciso realizar un análisis detallado para observar un incremento de la frecuencia y magnitud de los robos de tarjetas de crédito e identidades sufridos por minoristas, comerciantes y bancos. Un rápido vistazo a los principales periódicos revela que existen importantes puntos ciegos en las infraestructuras de seguridad de las organizaciones que comprometen la seguridad de los datos de clientes y consumidores.

II. Sinopsis de la norma PCI DSS

UNIVERSIDAD DE LIMA

La norma PCI DSS

- La norma resultante es la PCI DSS (Payment Card Industry Data Security Standard), desarrollada por VISA.
- PCI es un conjunto de requisitos de seguridad de datos y red para las empresas que tramitan transacciones realizadas con tarjetas de crédito (como minoristas, compañías de seguros, etc.) destinado a proteger la información confidencial del titular de la tarjeta.

Requisitos de la norma PCI DSS

- La norma PCI describe seis objetivos de control de la seguridad de red relativamente amplios:

1. Construir y mantener una red segura
2. Proteger los datos del titular de la tarjeta
3. Mantener el programa VA (Antivirus)
4. Implantar medidas de control de acceso seguras
5. Monitorizar y comprobar las redes regularmente
6. Mantener una política de seguridad de la información

- Estos 6 objetivos de control están compuestos por 12 requisitos más detallados.

UNIVERSIDAD DE LIMA

Resumen de requerimientos

Construir Y Mantener Redes Seguras	1. Instalar y mantener configuraciones de firewall para proteger la información 2. No usar contraseñas o parámetros de seguridad provistos por suplidores
Proteger La Información Del Tarjetahabiente	3. Proteger información almacenada 4. Cifrar datos de tarjetahabientes e información sensitiva al enviarla por redes públicas
Establecer Programas De Pruebas De Vulnerabilidades	5. Usar y actualizar regularmente programas de antivirus 6. Desarrollar y mantener sistemas y aplicativos seguros
Implementar Medidas Fuertes De Control De Acceso	7. Restringir acceso a información de acuerdo a reglas del negocio 8. Asignar IDs únicos para cada persona con acceso a sistemas 9. Restringir acceso a la información de tarjetahabiente
Regularmente Monitorear Y Probar Acceso A La Red	10. Rastrear y monitorear todos los accesos a la red e información del tarjetahabiente 11. Regularmente probar sistemas y procedimientos de seguridad
Mantener Políticas De Seguridad De La Información	12. Establecer políticas dirigidas a la seguridad de la información

Aplicabilidad PCI DSS

Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago como comerciantes, procesadores, instituciones financieras y proveedores de servicios. La clave para saber si debes aplicar PCI DSS es si **almacenas, procesas o transmites** datos de cuenta (datos del titular de la tarjeta y datos de autenticación confidenciales)

Aplicabilidad PCI DSS

- El número de cuenta principal es el "dato principal" de los datos del titular de la tarjeta, que define si debemos asegurar nuestro entorno de datos del titular de tarjeta (CDE) según las PCI DSS.

Datos de cuentas	
Los datos de titulares de tarjetas incluyen:	**Los datos confidenciales de autenticación incluyen:**
▪ Número de cuenta principal (PAN) ▪ Nombre del titular de la tarjeta ▪ Fecha de vencimiento ▪ Código de servicio	▪ Contenido completo de la pista (datos de la banda magnética o datos equivalentes que están en un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Bloqueos de PIN

Alcance

- Los requisitos de seguridad de las PCI DSS se aplican a todos los componentes del sistema incluidos en el entorno de datos del titular de la tarjeta. El entorno de datos del titular de la tarjeta (CDE) consta de personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. El término “componentes del sistema” incluye dispositivos de red, servidores, dispositivos informáticos y aplicaciones.

Aplicabilidad PCI DSS

		Elemento de datos	Almacenamiento permitido	Datos almacenados ilegibles según el Requisito 3.4
Datos de cuentas	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí
		Nombre del titular de la tarjeta	Sí	No
		Código de servicio	Sí	No
		Fecha de vencimiento	Sí	No
	Datos confidenciales de autenticación[2]	Contenido completo de la pista[3]	No	No se pueden almacenar según el Requisito 3.2
		CAV2/CVC2/CVV2/CID[4]	No	No se pueden almacenar según el Requisito 3.2
		PIN/Bloqueo de PIN[5]	No	No se pueden almacenar según el Requisito 3.2

- Los Requisitos 3.3 y 3.4 de las PCI DSS sólo se aplican al PAN. Si el PAN se almacena con otros elementos de los datos del titular de la tarjeta, únicamente el PAN debe ser ilegible de acuerdo con el Requisito 3.4 de las PCI DSS.
- No se deben almacenar los datos confidenciales de autenticación después de la autorización, incluso si están cifrados. Esto se implementa aún cuando no haya PAN en el entorno. Las organizaciones deben comunicarse con sus adquirientes o, directamente, con las marcas de pago para saber si pueden almacenar los SAD (datos de autenticación confidenciales) antes de la autorización, durante cuánto tiempo y para conocer cualquier requisito relacionado con la protección y el uso.

UNIVERSIDAD DE LIMA

Alcance PCI DSS

- Los requisitos de seguridad de las PCI DSS se aplican a todos los **componentes del sistema incluidos en el entorno de datos del titular de la tarjeta. El entorno de datos del titular de la tarjeta (CDE)** consta de personas, procesos y tecnologías que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. El término "componentes del sistema" incluye dispositivos de red, servidores, dispositivos informáticos y aplicaciones.

Componentes de sistema

- Sistemas que ofrecen servicios de seguridad (por ejemplo, servidores de autenticación), que facilitan la segmentación (por ejemplo, *firewalls* internos) o que pueden afectar la seguridad del CDE (por ejemplo, servidores de resolución de nombres o de redireccionamiento web).
- Componentes de virtualización, como máquinas virtuales, interruptores/routers virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores.
- Los componentes de red incluyen, a modo de ejemplo, *firewalls*, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de red y otras aplicaciones de seguridad.
- Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, bases de datos, autenticación, correo electrónico, proxy, NTP (protocolo de tiempo de red) y DNS (servidor de nombre de dominio).
- Aplicaciones, que abarcan todas las aplicaciones compradas y personalizadas, incluso las aplicaciones internas y externas (por ejemplo, Internet).
- Cualquier otro componente o dispositivo ubicado en el CDE o conectado a este.

Recomendaciones sobre el alcance

- El primer paso de una evaluación de las PCI DSS es determinar con exactitud el alcance de la revisión.
- Por lo menos una vez al año y antes de la evaluación anual, la entidad evaluada deberá confirmar la exactitud del alcance de las PCI DSS al identificar todas las ubicaciones y los flujos de datos del titular de la tarjeta, e identificar todos los sistemas a los que se conectan o, si están en riesgo, podrían afectar al CDE (por ejemplo, los servidores de autenticación) para garantizar que se incluyan en el alcance de las PCI DSS. Todos los tipos de sistemas y ubicaciones deberán considerarse como parte del proceso de alcance, incluidos los sitios de copia de seguridad/recuperación y los sistemas de conmutación por error.
- Para confirmar la exactitud del CDE definido, realice lo siguiente:
  - La entidad evaluada identifica y documenta la existencia de todos los datos del titular de la tarjeta en su entorno, con la finalidad de verificar que no haya datos del titular de la tarjeta fuera del CDE actualmente definido.
  - Una vez que se hayan identificado y documentado todas las ubicaciones de los datos de los titulares de tarjetas, la entidad utiliza los resultados para verificar que el alcance de las PCI DSS sea apropiado (por ejemplo, los resultados pueden ser un diagrama o **un inventario de ubicaciones de datos de titulares de tarjetas**).
  - La entidad considera que todos los datos del titular de la tarjeta encontrados están dentro del alcance de la evaluación de las PCI DSS y forman parte del CDE. Si la entidad identifica los datos que no están actualmente en el CDE, o al CDE redefinido para incluir estos datos. se deberán eliminar de manera segura, migrar al CDE actualmente definido

Plantilla para la matriz de datos del tarjetahabiente

Cardholder Data Matrix
PCI DSS 3.2

ID	Descripción
PER	Personal
APP	Aplicaciones
SRV	Servidores y estaciones de trabajo
NET	Equipos de red y seguridad perimetral
SOP	Soportes (CD, papel, etc.)
CAN	Canales
INS	Instalaciones físicas
TER	Terceros (Proveedores)
PCI	Ubicación datos PCI DSS

¿Superintendencia de Banca, Seguros y AFP?

- La Superintendencia de Banca, Seguros y AFP es el organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. ***Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP.***

UNIVERSIDAD DE LIMA

Reglamento de Tarjetas de Débito y Crédito

- El 30 de Octubre del 2013 aprueba por resolución 6523-2013 el Reglamento de Tarjetas de Debito y de Crédito

UNIVERSIDAD DE LIMA

Reglamento de Tarjetas de Débito y Crédito

- El Reglamento tiene un apartado de medidas de seguridad sobre las tarjetas de crédito y débito, esencialmente en los artículos:

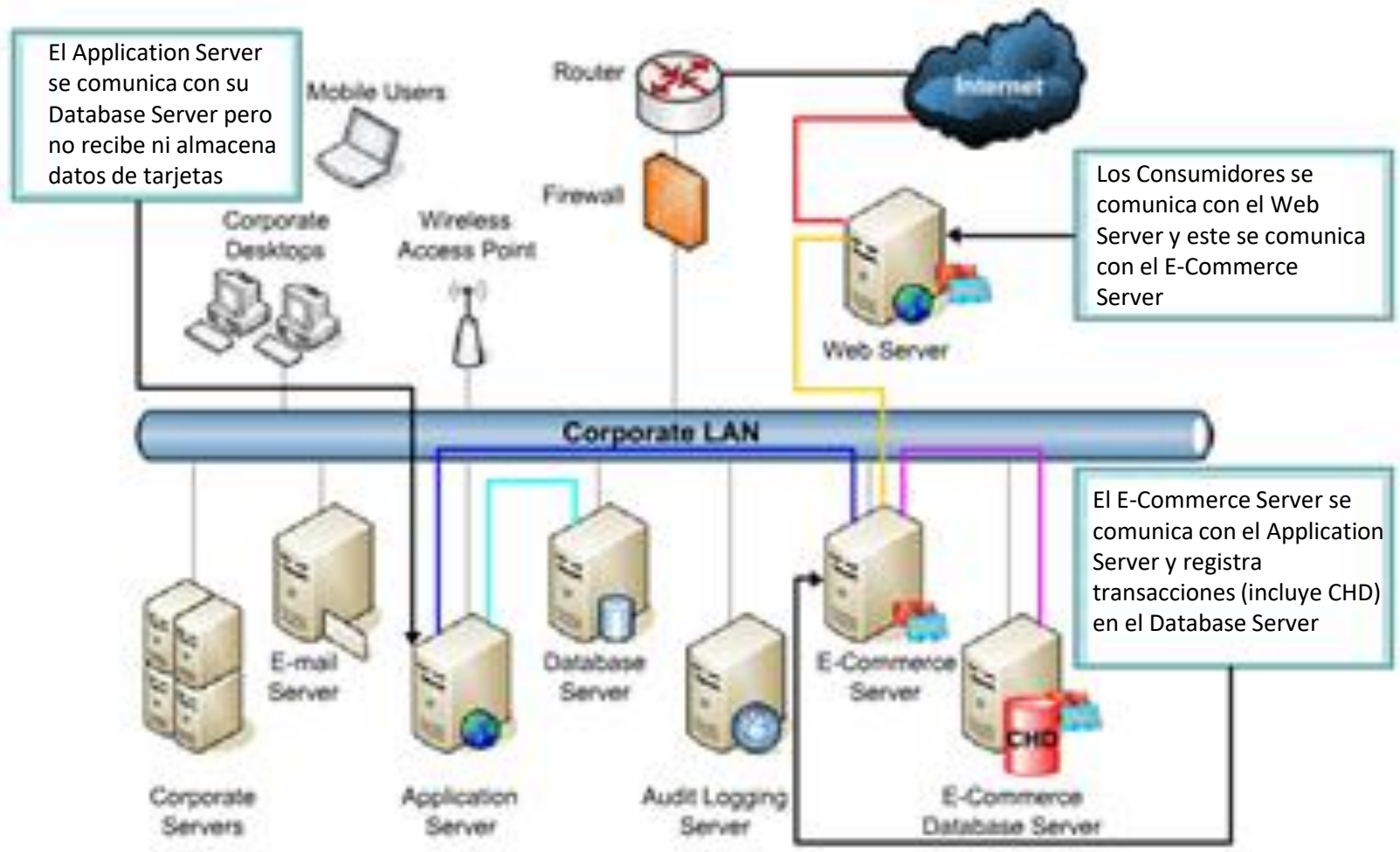
  Artículo 15°.- Medidas de seguridad incorporadas en las tarjetas
  Artículo 16°.- Medidas de seguridad respecto a los usuarios
  Artículo 17°.- Medidas de seguridad respecto al monitoreo y realización de las operaciones
  Artículo 18°.- Medidas en materia de seguridad de la información (PCI DSS)
  Artículo 19°.- Medidas de seguridad en los negocios afiliados
  Artículo 20°.- Requerimientos de seguridad en caso de subcontratación

UNIVERSIDAD DE LIMA

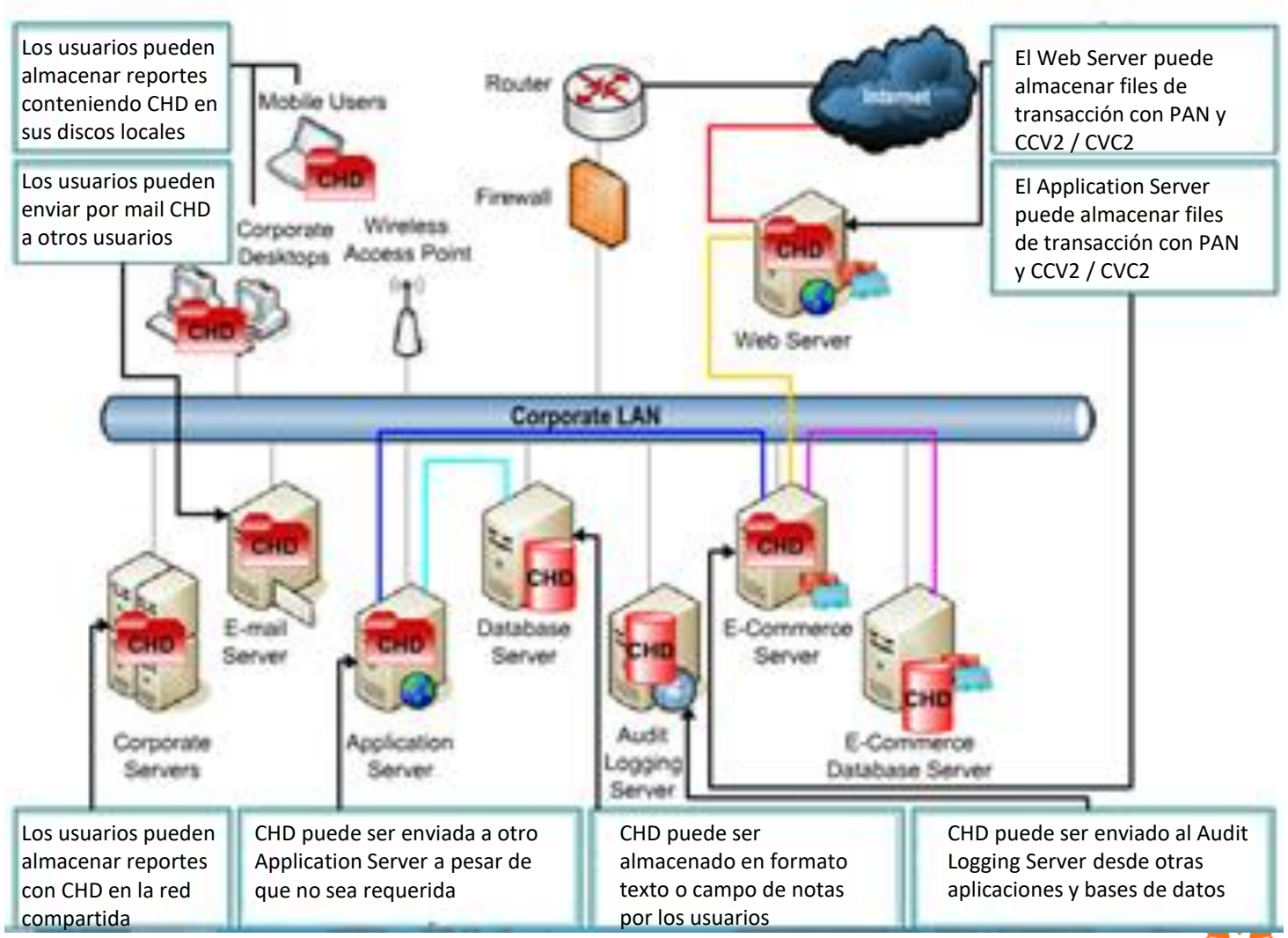
¿Dónde se almacenan los datos del tarjetahabietne?

- Los datos de los tarjetahabientes se almacenan en lugares conocidos y desconocidos en la mayoría de las redes.
- Los datos de los tarjetahabientes pueden "escaparse" de lugares de almacenamiento conocidos.
- Teniendo un buen inventario podría ser el punto de partida para identificar las ubicaciones de almacenamiento de datos de titulares de tarjetas.
- Una búsqueda exhaustiva se debe hacer de todos los sistemas en la red para identificar datos del tarjetahabiente y tracks.

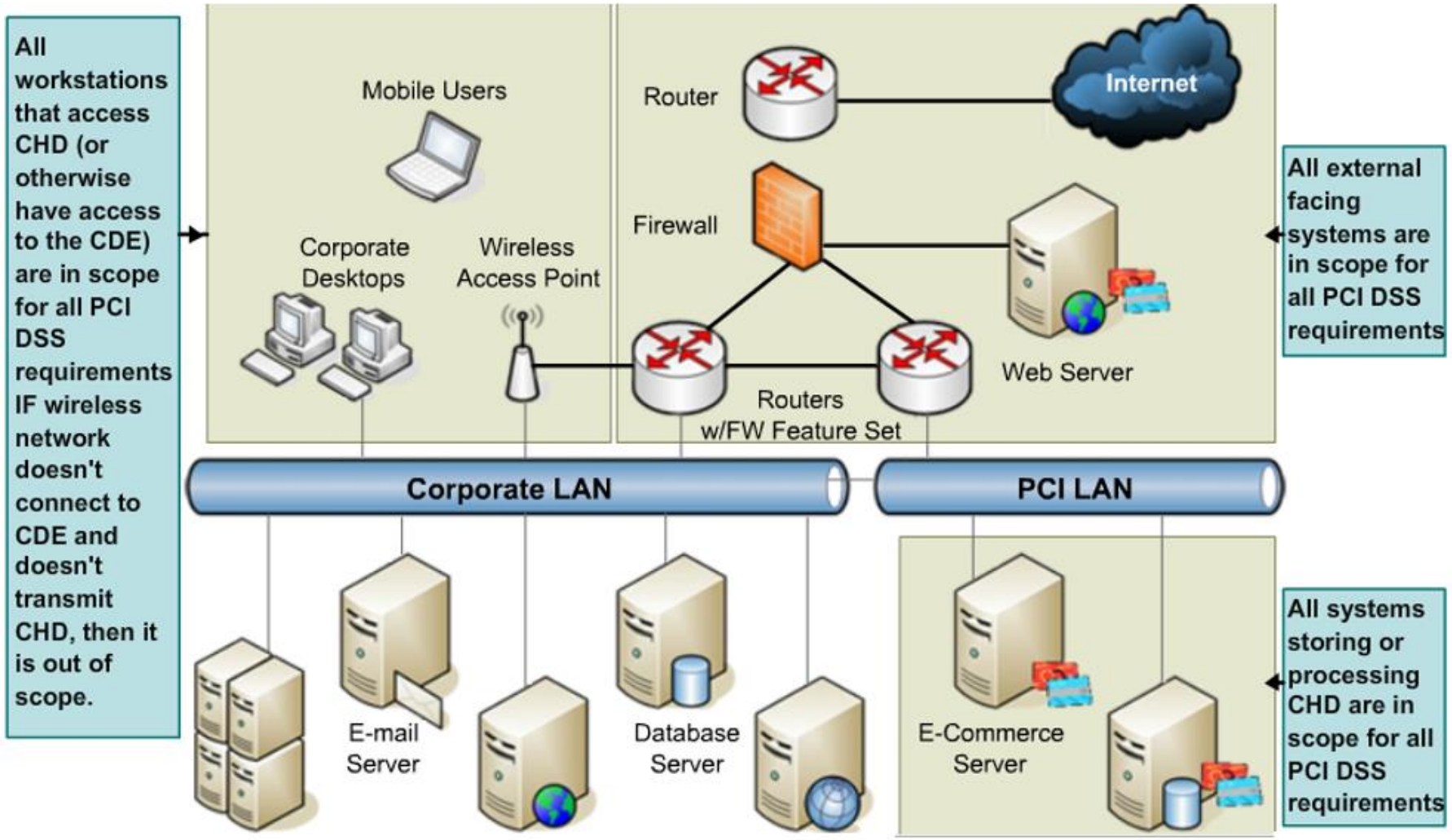
Caso de estudio



Caso de estudio



Caso de estudio: Segmentación



III. Los REQUISITOS PCI DSS

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

Desarrolle y mantenga redes y sistemas seguros

Requisito 1:	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta
Requisito 2:	No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores

Pasos recomendados:

- Sistemas no conectados a Internet
- Configuración de Firewall específica para cada sistema y cliente
- Lista de puertos TCP/UDP
- Cuentas y contraseñas específicos por sistema

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

Proteger los datos del titular de la tarjeta

Requisito 3:	Proteja los datos del titular de la tarjeta que fueron almacenados
Requisito 4:	Cifrar la transmisión de los datos del titular de la tarjeta en las redes publicas abiertas

Pasos recomendados:	▪ Encriptación de los medios End-to-End, AES 256 ▪ Cambio periódico de claves con gestor interno de claves ▪ Comunicación de cliente Segura (https, sftp, ssl) ▪ Control de Privacidad ▪ Pausa de la grabación

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

Maintain a Vulnerability Management Program

Requisito 5:	Utilizar y actualizar con regularidad los programas o software antivirus
Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras

Pasos recomendados:

- Programa de soporte de actualización de Parches y Software
- Certificación y soporte de Antivirus
- Inspección de sistemas por expertos independientes de seguridad

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

Implementar medidas sólidas de control de acceso

Requisito 7:	Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
Requisito 8:	Identifique y autentifique el acceso a los componentes del sistema
Requisito 9:	Restringir el acceso físico a los datos del titular de la tarjeta

Pasos recomendados:	▪ Soporte de LDAP ▪ Administración de usuarios basados en Perfiles ▪ Audit trail ▪ Integridad doble para todas las aplicaciones

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

Supervisar y evaluar las redes con regularidad

Requisito 10:	Rastree y supervise todos los accesos a los recursos de red a los datos de los titulares de las tarjetas
Requisito 11:	Pruebe con regularidad los sistemas y procesos de seguridad.

Pasos recomendados:

- Monitorización sobre: Login, Busqueda, Reproducción, Monitorización, Configuración,...
- Audit trail

UNIVERSIDAD DE LIMA

PCI-DSS: Requisitos

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

UNIVERSIDAD DE LIMA

PCI-DSS; Seis metas y doce requisitos (sumario)

Desarrolle y mantenga redes y sistemas seguros	Requisito 1:	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta
	Requisito 2:	No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	Requisito 3:	Proteja los datos del titular de la tarjeta que fueron almacenados
	Requisito 4:	Cifrar la transmisión de los datos del titular de la tarjeta en las redes publicas abiertas
Mantener un programa de administración de vulnerabilidad	Requisito 5:	Utilizar y actualizar con regularidad los programas o software antivirus
	Requisito 6:	Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	Requisito 7:	Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	Requisito 8:	Identifique y autentifique el acceso a los componentes del sistema
	Requisito 9:	Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	Requisito 10:	Rastree y supervise todos los accesos a los recursos de red a los datos de los titulares de las tarjetas
	Requisito 11:	Pruebe con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	Requisito 12:	Mantenga una política que aborde la seguridad de la información para todo el personal.

UNIVERSIDAD DE LIMA

IV. conclusiones

UNIVERSIDAD DE LIMA