Ingeniería de Sistemas

PCI: Protección de transacciones con tarjetas de pago

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

Flujo de una transacción de pago y PCI

Cada transacción realizada con una tarjeta de pago consiste en dos pasos:
Flujo de transacción, Compensación y Liquidación.

Flujo de la Transacción

el cliente desliza la tarjeta en un POS o introduce los datos en el portal web.

El establecimiento comercial entonces almacena el tipo de tarjeta, número de cuenta, fecha de expiración y otros códigos de identificación y seguridad.

La información es enviada al comerciante-comprador (merchant-acquirer : empresa otorgó la tarjeta)

El emisor de la tarjeta verifica entonces el estado de la cuenta en sus bases de datos y responde al comprador. Este reenvía el código de autorización al equipo terminal donde se inició el proceso.

Compensación y Liquidación.

el comprador recibe los datos por parte del comerciante

el comerciante y los envía a la red de pagos apropiada (Visa, MasterCard, etc) en donde se encamina directamente al emisor de la tarjeta.

Emisor finalmente realiza el cobro al usuario y retorna el pago respectivo, descontando sus respectivos impuestos.

Ver esquema

UNIVERSIDAD DE LIMA

Proceso de Autorización

El Tarjetahabiente ingresa su Tarjeta de Pago en el Comercio

El Adquirente consulta con la red de la Marca de Tarjeta para determinar al Emisor

La red de la Marca de tarjeta determina al Emisor y requiere la aprobación del pago

El Emisor aprueba el Pago

El tarjetahabiente completa el pago y recibe su comprobante

El Adquirente envía la aprobación al Comercio

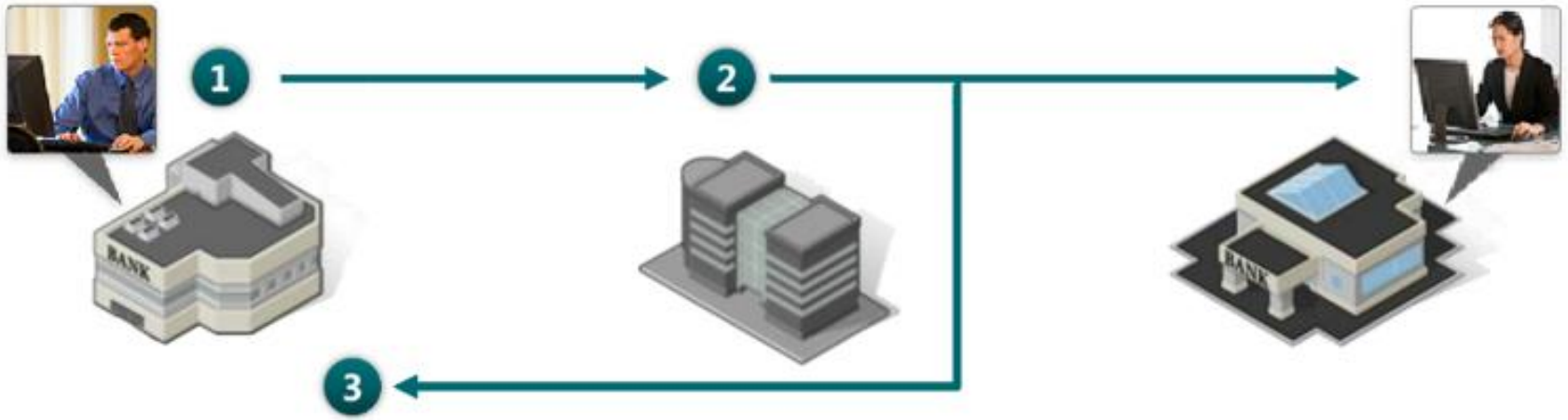
La red de la Marca de Tarjeta envía la aprobación al Adquirente

UNIVERSIDAD DE LIMA

Proceso de Compensación

El Adquirente envía la información de pago a la red de la Marca de Tarjeta

La red de la Marca de Tarjeta envía la información de pago al Emisor, quien prepara los datos del estado de cuenta del tarjetahabiente



La red de la Marca de Tarjeta provee los datos de conciliación al Adquirente

Este Proceso, se efectua generalmente dentro de 1 día

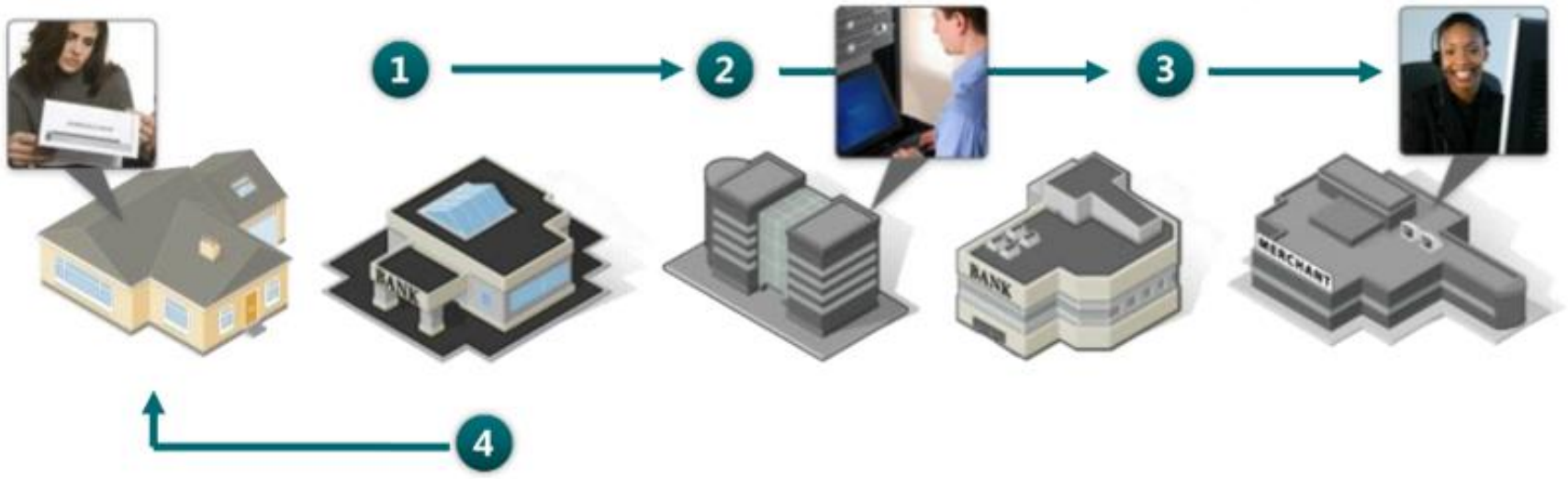
UNIVERSIDAD DE LIMA

Proceso de Liquidación

El Emisor determinan el Adquirente mediante la red de la Marca de Tarjeta

El Emisor envía los pagos al Banco pagador del Comercio (Adquirente)

El Adquirente paga al Comercio por los pagos efectuados por los tarjetahabientes

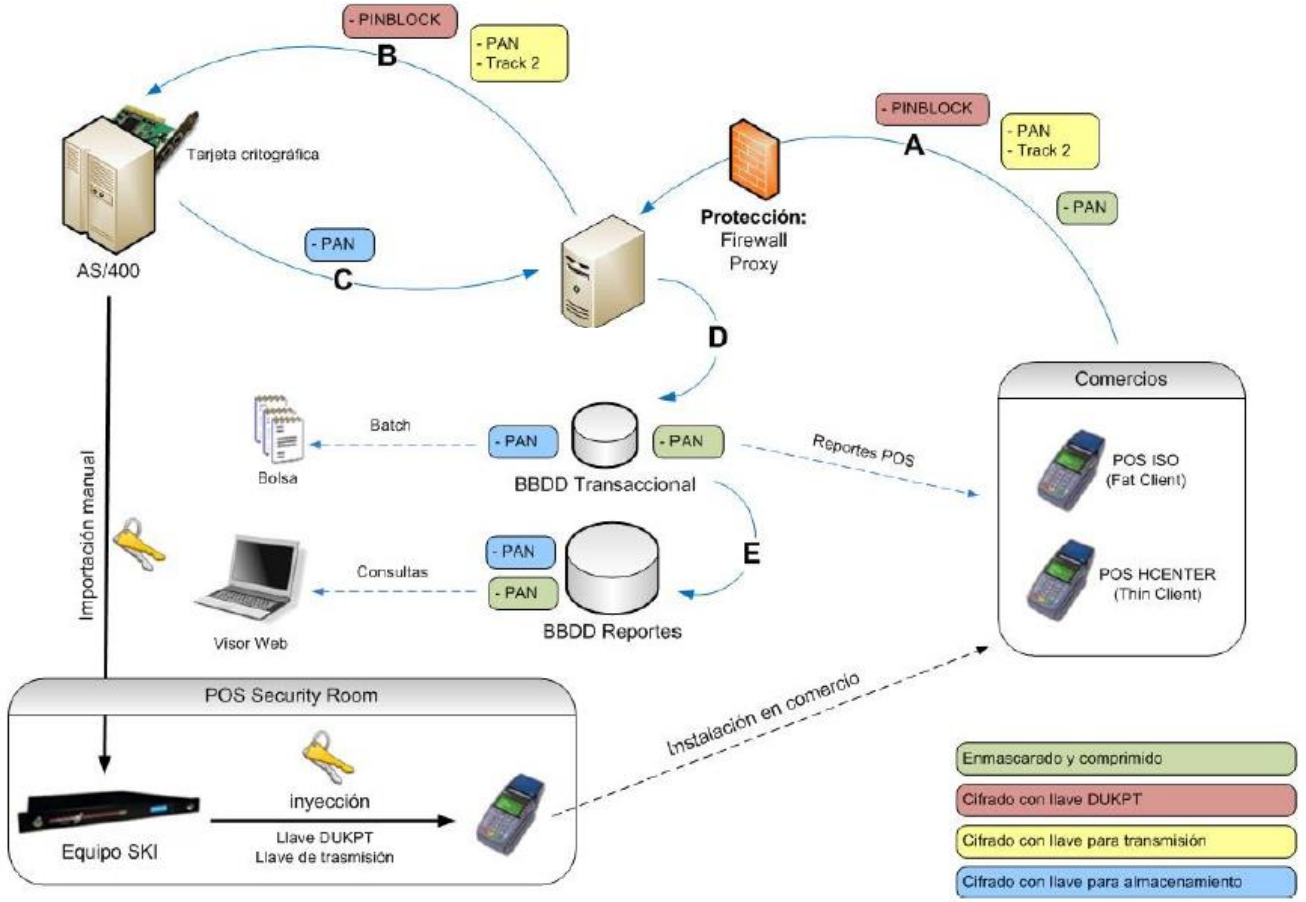


El Emisor emite las facturas o resúmenes de pago al Tarjetahabiente

Este proceso, se efectua generalmente dentro de 2 días

UNIVERSIDAD DE LIMA

Ejemplo de flujo de datos de tarjeta



- El flujo de datos tiene que ser a nivel de grafico y escrito.

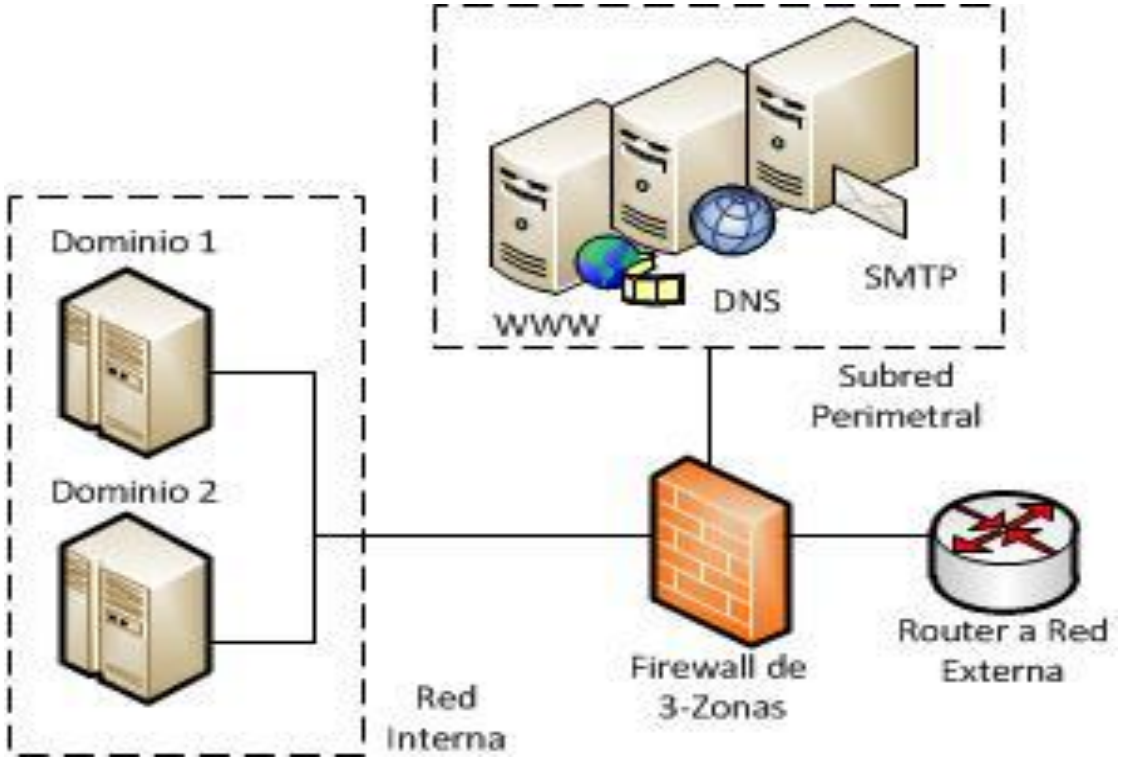
UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

1.Construir y Mantener una Red Segura

PCI DSS requiere que se tenga un Firewall configurado para proteger su propia red, y por ende, los datos de los portadores de tarjetas de pago.

Firewall de tres áreas: interna donde está almacenada la información sensible (INS – Internal Network Zone), Perimetral (DMZ, Demilitarized Zone) en donde están los servidores de acceso externo y la zona externa, como se observa en la figura 2. Cada interconexión de zonas debe estar supervisada y controlada por un juego de reglas en el Firewall. Por ejemplo, cualquier tráfico de la zona externa a una zona interna debe ser denegado y bloqueado.

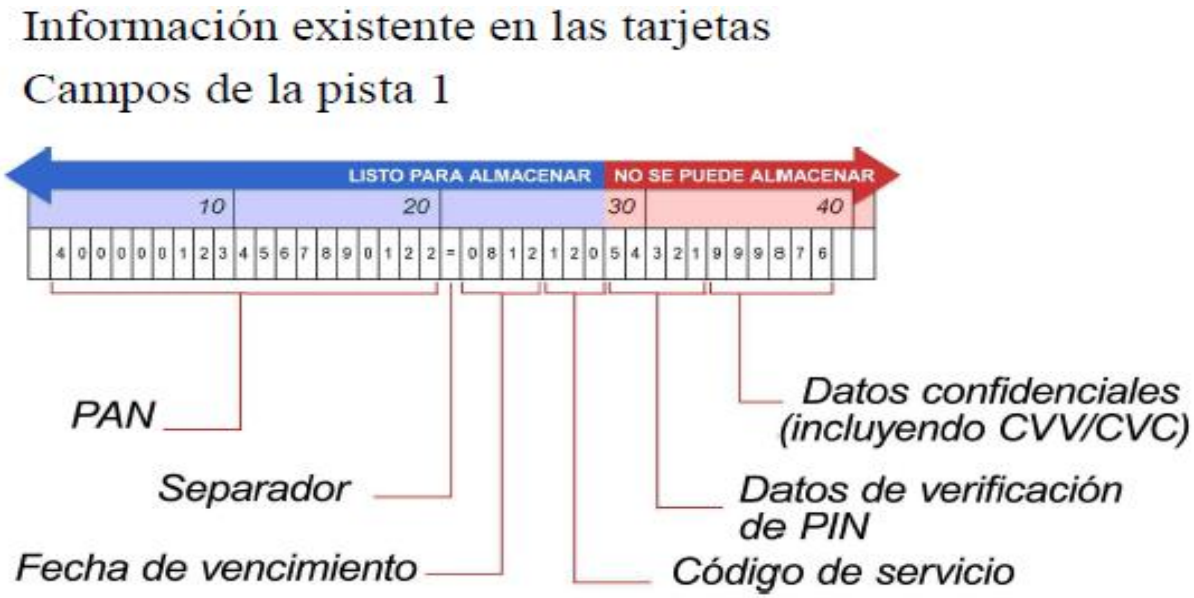


PCI recomienda no utilizar cualquier configuración por defecto de los equipos, como contraseñas y SSID de conexiones inalámbricas que deben usar además encriptación.

UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

Proteger Información del Portador de las Tarjetas



Almacenamiento: se debe limitar la información almacenada a el menor tiempo posible de acuerdo las necesidades del negocio y restricciones legales, y no se debe nunca almacenar la información de la cinta magnética o códigos de verificación ni números de identificación personal (PIN). La información que sea almacenada debe estar encriptado .

UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

2.Proteger Información del Portador de las Tarjetas

Comunicaciones: Durante la transmisión de esta información, se debe utilizar protocolos de seguridad y criptografía fuerte como Internet Protocol Security (IPSEC) y SSL/TLS. Se recomienda usar librerías de criptografía como AES y 3DES. En comunicaciones inalámbricas, además se requiere protocolos como WPA, WPA2, VPN y SSL.

UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

3.Mantener un Programa de Gestión de Vulnerabilidades

Software malicioso, como virus, gusanos y trojanos pueden dar acceso a personas malintencionadas. Estas pueden acceder incluso por medios legítimos como email, dispositivos portátiles o unidades de disco externos. Se recomienda usar software de seguridad como Antivirus para llevar un registro de estas acciones y evitar las acciones más comunes.

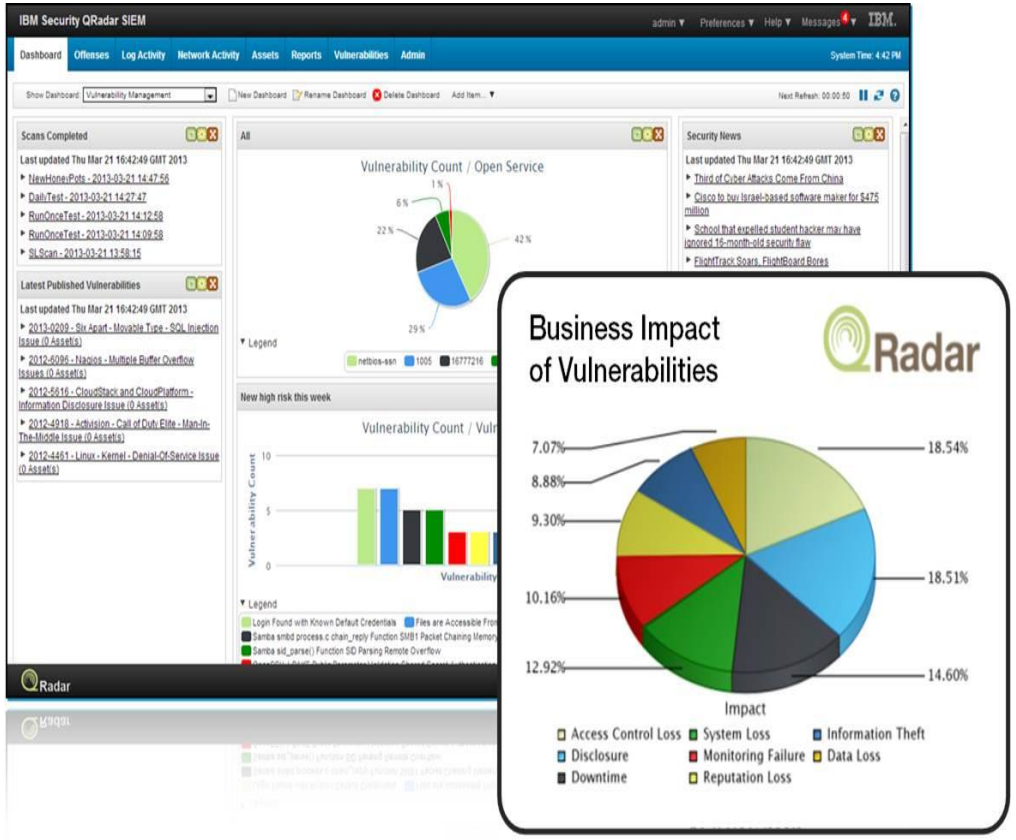
Seguir el *Open Web Application Security Project Guide*, con el fin de validar que se evitan las vulnerabilidades mas conocidas como validación de datos de entrada, ataques cross-site scripting, desbordamientos de memoria, entre otras.

UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

4.Implementar Sistemas de Acceso Seguro

Cualquier acceso a información sensible debe ser controlado y autorizado solamente a quienes lo necesiten y en el nivel requerido. Además, cada usuario debe contar un ID que permite ser auditado sobre sus acciones. Cada ID, como nombre de usuario, contraseña, token o información biométrica deben ser encriptados antes de ser transmitidos y cada cambio realizado debe ser almacenado en un log.



5. Monitoreo Regular y Prueba de Redes

PCI DSS demanda que todo acceso a información sensible debe ser seguida y monitoreada en logs. Estos permiten determinar las acciones de todas las personas y determinar las razones si algo falla. Estos archivos deben almacenar accesos fallidos tratando de usar privilegios de administradores y asociarlos con los mecanismos de identificación.

UNIVERSIDAD DE LIMA

Estándar de Seguridad De Datos Para Pagos Con Tarjeta – PCI DSS
Objetivos de control

6. Mantener una Política de Seguridad de Información

Define la sensibilidad de la información y la responsabilidad de los trabajadores en la protección de la información que tienen a cargo.

Se deben desarrollar políticas de uso para los empleados que usen dispositivos críticos o tecnológicos que puedan presentar algún tipo de amenaza, como tecnologías inalámbricas, dispositivos portátiles, memorias removibles, PDAs e incluso correo electrónico. Cada uno de estos debe tener una autenticación para ser utilizadas, y esta solo se debe dar después de haber sido inspeccionados y entendido la importancia de ser aprobadas para la ejecución de las labores del empleado. Adicionalmente, cada dispositivo debe ser almacenado en una base de datos con los datos de quien lo utiliza para poder dar seguimiento a sus acciones.

UNIVERSIDAD DE LIMA