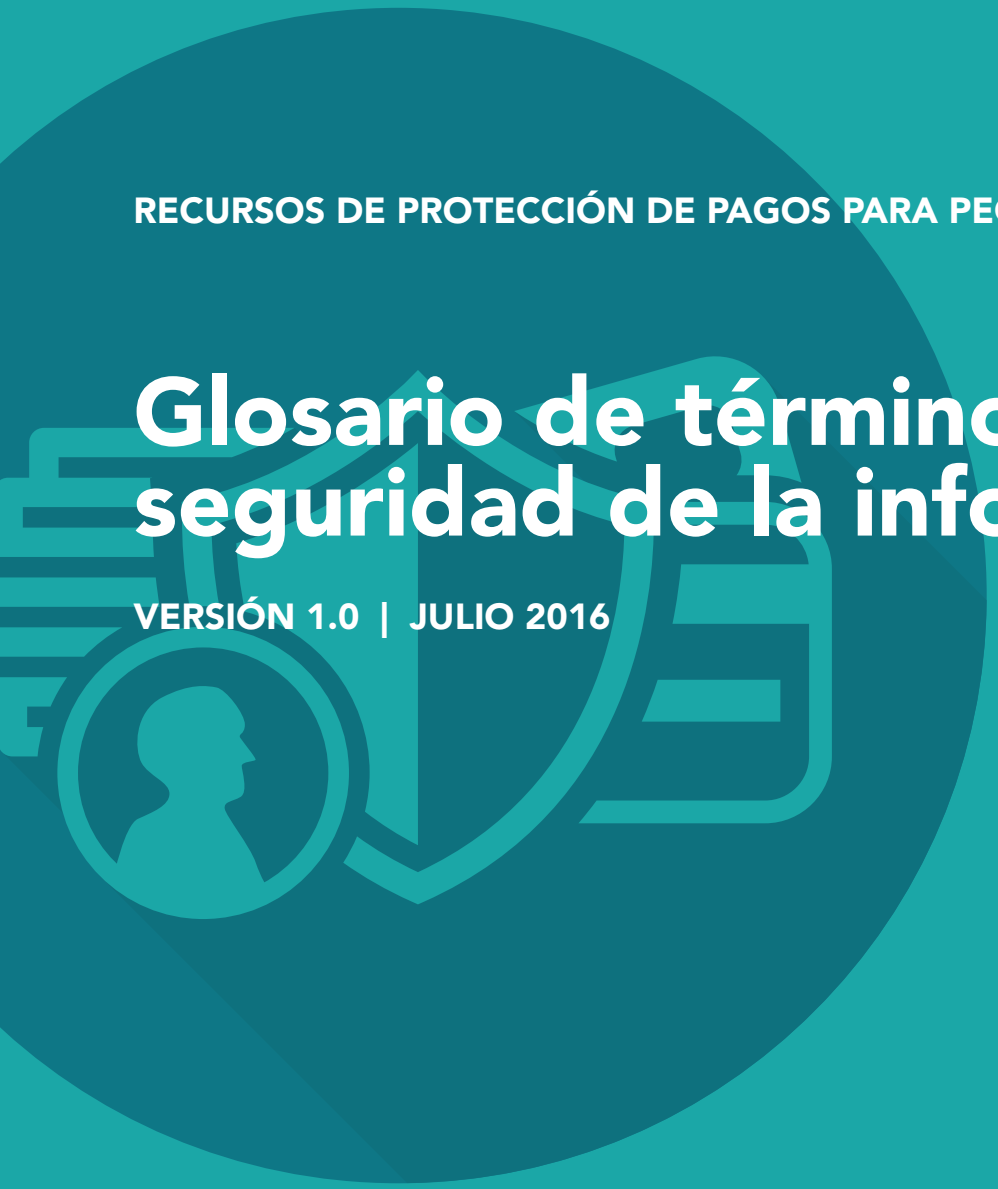

RECURSOS DE PROTECCIÓN DE PAGOS PARA PEQUEÑOS COMERCIANTES

Glosario de términos sobre pagos e seguridad de la información

VERSIÓN 1.0 | JULIO 2016

PCI Security Standards Council®

Introducción

Este *Glosario de términos sobre pagos y seguridad de la información* es un complemento de la *Guía de pagos seguros*, que forma parte de los Recursos de protección de pagos para pequeños comerciantes. Su objetivo es explicar los términos relevantes de la seguridad de la información y la Industria de tarjetas de pago (PCI) de manera simple y fácil de entender.

Las definiciones para los términos marcados con un asterisco (*) se basan en o derivan de las definiciones en la *Norma de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI)* y *Norma de seguridad de datos para las aplicaciones de pago (PA-DSS): Glosario de Términos, Abreviaturas y Acrónimos*, Versión 3.2, con fecha de abril de 2016.

Consulte la *Guía de pagos seguros* y los otros Recursos de protección de pagos para pequeños comerciantes en los siguientes sitios:

RECURSO	URL
Guía de pagos seguros	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Sistemas de pago comunes	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Preguntas para hacerles a sus proveedores	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

Nota:
La última versión de la *Norma de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI) y Norma de seguridad de datos para las aplicaciones de pago (PA-DSS): Glosario de Términos, Abreviaturas y Acrónimos* se considera la fuente autorizada y debe consultarse para obtener definiciones completas y actuales de la PCI DSS y la PA-DSS.

Glosario

TÉRMINO	DEFINICIÓN
Adquirente *	Consulte *Banco comercial* y *Procesador de pago*.
Software antivirus *	Programa de software que detecta, elimina y protege contra los programas maliciosos (también denominados "malware"), incluidos virus, gusanos, troyanos o caballos troyanos, spyware, adware y rootkits. También se lo conoce como "software contra malware".
Aplicación *	Programa de software o grupo de programas que se ejecuta en una computadora, teléfono inteligente, tableta, servidor interno o servidor web.
Proveedor aprobado de escaneo (ASV) *	Compañía aprobada por el PCI Security Standards Council para realizar servicios de escaneo e identificar debilidades comunes en la configuración del sistema. Consulte también *ASV*.
ASV *	Acrónimo de "Approved Scanning Vendor" (proveedor aprobado de escaneo).
Autenticación *	Proceso para verificar la identidad de un individuo, dispositivo o proceso. Por lo general, la autenticación ocurre a través del uso de uno o más factores de autenticación, tales como: • Algo que usted sabe, como una contraseña o frase de acceso • Algo que usted tiene, como un dispositivo token o tarjeta inteligente • Algo que usted es, como un sistema biométrico
Autorización *	En una transacción con tarjeta de pago, la autorización ocurre cuando un comerciante recibe la aprobación de la transacción después de que el adquirente valida la transacción con el emisor/procesador.
Número de identificación bancaria (BIN)	Los seis primeros dígitos (o más) del número de una tarjeta de pago que identifica a la institución financiera que emitió la tarjeta de pago al titular de esta.
Necesidad de saber que tenga la empresa	El principio para acceder a los sistemas o datos se otorga según la necesidad comercial del usuario, solo lo que es necesario para el desempeño laboral de un usuario.
Datos de la tarjeta/Datos de la tarjeta del cliente *	Como requisito mínimo, los datos de la tarjeta incluyen el número de cuenta principal (PAN) y además pueden incluir la fecha de vencimiento y el nombre del titular de tarjeta. El PAN se encuentra en el anverso de la tarjeta y codificado en la banda magnética de la tarjeta o en el chip inserto en su interior. También conocido como datos del titular de la tarjeta. Además, consulte los *Datos confidenciales de autenticación para ver cuáles son otros elementos de datos que pueden ser parte de una transacción de pago, pero que no deben almacenarse después de que se autoriza la transacción*.
Chip	También denominado "chip de tipo EMV". El microprocesador (o "chip") en una tarjeta de pago que se utiliza cuando se procesan transacciones según las especificaciones internacionales para las transacciones de EMV.

Glosario

TÉRMINO	DEFINICIÓN
Chip y PIN	Proceso de verificación en el que un consumidor ingresa su PIN en un terminal de pago habilitado para chip de tipo EMV cuando compra productos o servicios.
Chip y firma	Proceso de verificación donde un consumidor usa su firma en un terminal de pago habilitado para chip de tipo EMV cuando compra productos o servicios.
Credencial	Información que se utiliza para identificar y autenticar a un usuario para el acceso a un sistema. Por ejemplo, las credenciales son generalmente la contraseña y el nombre de usuario. Las credenciales pueden incluir un huella dactilar, un escaneo de retina o un número generado por única vez por un "generador de tokens" portátil. La seguridad es más sólida cuando el acceso requiere varias credenciales.
Ataque cibernético	Cualquier tipo de maniobra ofensiva para irrumpir en una computadora o en un sistema. Los ataques cibernéticos pueden variar desde instalar un spyware en una computadora, irrumpir en un sistema de pago para robar datos de la tarjeta o intentar dañar una infraestructura crítica como una red de energía eléctrica.
Filtración de datos	Una filtración de datos es un incidente en el cual una parte no autorizada posiblemente pueda ver, robar o utilizar datos confidenciales. Las filtraciones de datos pueden involucrar datos de la tarjeta, información personal de salud (personal health information, PHI), información de identificación personal (personally identifiable information, PII), secretos comerciales o propiedad intelectual, etc.
Contraseña predeterminada	Una contraseña simple que viene con un software o hardware nuevo. Contraseñas predeterminadas (como "admin" o "contraseña" o "123456") son fáciles de adivinar y generalmente están disponibles a través de una búsqueda en línea. Aparecen como un marcador de posición y no ofrecen ninguna seguridad real (y deben cambiarse por una contraseña más segura después de la instalación de un nuevo software o hardware).
Caja registradora electrónica (ECR)	Un dispositivo que registra y calcula transacciones y puede imprimir recibos, pero no acepta pagos con tarjeta del cliente. También denominada "till" (caja registradora).
Cifrado	Proceso que emplea la criptografía para convertir información en un formato matemático que no se puede utilizar, salvo aquellas personas que tengan una clave digital específica. El uso de un cifrado protege la información y ya no tiene valor para los delincuentes. Consulte también *Criptografía*.
Firewall *	Hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea la comunicación entre computadoras o redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios.
Investigador forense	Los investigadores forenses de la PCI (Forensic Investigators, PFI) son compañías aprobadas por el Consejo de la PCI para ayudar a determinar cuándo y cómo se produjo una filtración de datos de la tarjeta. Ellos realizan investigaciones dentro de la industria financiera utilizando herramientas y metodologías de investigación comprobadas. Además, trabajan con autoridades competentes responsables de exigir la ley para respaldar a las partes interesadas con cualquier investigación de delitos resultante.

Glosario

TÉRMINO	DEFINICIÓN
Hacker	Una persona u organización que intenta evadir las medidas de seguridad de los sistemas de computadoras para obtener control y acceso a estas. Generalmente, esto se realiza con el fin de robar datos de la tarjeta.
Proveedor de hosting *	Ofrece varios servicios a los comerciantes y otros proveedores de servicios, donde se "alojan" los datos de sus clientes o residentes en los servidores del proveedor. Los servicios típicos incluyen espacio compartido para varios comerciantes en un servidor y ofrecen un servidor exclusivo para un comerciante, o aplicaciones web como un sitio web como opciones de "carrito de compras".
Terminal de pago integrado	Un terminal de pago y una caja registradora electrónica en un solo dispositivo que acepta pagos, registra y calcula transacciones e imprime recibos.
Revendedor/Integrador	Un integrador/revendedor es una compañía que implementa, configura o respalda terminales de pago, sistemas de pago o aplicaciones de pago para comerciantes. Además, estas compañías pueden vender los dispositivos de pago o las aplicaciones como parte de su servicio. Además, consulte *Integrador o revendedor certificado (QIR)*.
Registro *	Un archivo que se crea automáticamente cuando ciertos eventos predefinidos (generalmente relacionados con la seguridad) ocurren dentro de una red o un sistema de computadoras. Los datos del registro incluyen el sello de fecha/hora, la descripción del evento e información única de ese evento. Estos archivos son útiles para solucionar problemas técnicos o una investigación de filtración de datos. También denominado "registro de auditoría" o "pista de auditoría".
Malware *	Software malicioso diseñado para infiltrarse en un sistema informático con la intención de robar datos, dañar aplicaciones o el sistema operativo. Dicho software generalmente ingresa a una red durante muchas actividades comerciales aprobadas como envíos de correos electrónicos o navegación en sitios web. Ejemplos de malware son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.
Banco comercial *	Un banco comercial o una institución financiera que procesa pagos con tarjeta de débito/crédito en nombre de los comerciantes. También denominado "adquirente", "banco adquirente", "procesador de tarjeta" o "procesador de pago". Consulte también *Procesador de pago*.
Dispositivo móvil	Término general que se utiliza para definir una clase de dispositivos electrónicos como teléfonos inteligentes y tabletas que son pequeños, portátiles y que pueden conectarse a las redes informáticas de manera inalámbrica.
Aceptación de pago móvil	Uso de un dispositivo móvil para aceptar y procesar transacciones de pago. Generalmente, el dispositivo móvil se utiliza con un accesorio de lector de tarjetas disponible en el mercado.
Autenticación de múltiples factores *	Método de autenticación de un usuario mediante la comprobación de dos o más factores. Estos factores incluyen algo que el usuario posee (como una tarjeta inteligente o un dongle), algo que sabe (como una contraseña, frase de seguridad o PIN) o algo que el usuario es o algo que hace (como las huellas dactilares y otros elementos biométricos, entre otros).
Red *	Dos o más computadoras interconectadas a través de un medio físico o inalámbrico.

Glosario

TÉRMINO	DEFINICIÓN
Sistema operativo *	Software de un sistema informático a cargo de compartir recursos informáticos, y administrar y coordinar todas las actividades informáticas. Algunos de ellos son Microsoft Windows, Apple OSX, iOS, Android, Linux y UNIX.
P2PE	Acrónimo de "Point-to-Point-Encryption" de la Norma de cifrado de punto a punto del Consejo de la PCI. Consulte los detalles en *www.pcisecuritystandards.org*.
PA-DSS *	Acrónimo de "Payment Application Data Security Standard" (Norma de Seguridad de Datos para las Aplicaciones de Pago) del Consejo de la PCI. Consulte los detalles en *www.pcisecuritystandards.org*.
Contraseña *	Una palabra, una frase o una serie de caracteres que se utilizan para autenticar a un usuario. Cuando se combina con el nombre de usuario, la contraseña tiene como objetivo comprobar la identidad del usuario para acceder a los recursos informáticos.
Parche *	Actualización de un software existente que agrega funcionalidad o corrige un defecto (o "error").
Aplicación de pago *	Relacionada con la PA-DSS, una aplicación de software que almacena, procesa o transmite datos del titular de la tarjeta como parte de la autorización o liquidación de transacciones de pago.
Proveedor de la aplicación de pago	Una entidad que vende, distribuye u otorga licencias de una aplicación de pago a los revendedores/integradores de los POS para la integración en sistemas de pago del comerciante o directamente para la instalación y el uso personal del comerciante.
Middleware de pago	Un término general para definir un software que conecta dos o más aplicaciones de pago que quizá no estén relacionadas entre sí. Por ejemplo, puede transmitir datos de la tarjeta entre una aplicación en un terminal de pago y otros sistemas del comerciante que envían datos de la tarjeta a un procesador.
Procesador de pago *	Entidad contratada por comerciantes para manejar transacciones con tarjetas de pago en su nombre. Si bien los procesadores de pago generalmente ofrecen servicios de adquirente, los procesadores de pago no son considerados adquirientes (bancos comerciales), a menos que así lo defina una marca de tarjeta de pago. También denominado "puerta de enlace para pagos" o "proveedor de servicios de pago" (PSP). Consulte también *Banco comercial*.
Sistema de pago	Abarca el proceso completo de la aceptación de pagos con tarjeta en una tienda minorista de un comerciante (incluye tiendas/comercios y escaparates de comercio electrónico). Este puede incluir un terminal de pago, una caja registradora electrónica, otros dispositivos o sistemas conectados al terminal de pago (por ejemplo, Wi-Fi para conectividad o una computadora que se utilice para inventario), servidores con componentes de comercio electrónico como páginas de pagos, y las conexiones con un banco comercial.
Proveedor de sistema de pago	Un proveedor que vende, distribuye u otorga una licencia para una solución de pago completa a un comerciante. La solución abarca el hardware y el software necesarios para manejar pagos dentro de la tienda y ofrece un método para conectarse a un procesador de pago.
Terminal de pago	Dispositivo de hardware que se utiliza para aceptar los pagos con tarjeta del cliente ya sea al pasar, deslizar, insertar o teclear el número de la tarjeta. También denominado "terminal de puntos de venta (POS)" "máquina de tarjeta de crédito" o "terminal de proceso rápido de datos (PDQ)".

Glosario

TÉRMINO	DEFINICIÓN
PCI *	Acrónimo de "Payment Card Industry" (Industria de tarjetas de pago).
PCI DSS *	Acrónimo de "Payment Card Industry Data Security Standard" (Norma de seguridad de datos de la Industria de tarjetas de pago) del Consejo de la PCI. Consulte los detalles en *www.pcisecuritystandards.org*.
Cumplimiento con la PCI DSS	Cumplir con todos los requisitos correspondientes de la PCI DSS vigente, de manera constante a través de un enfoque de actividades habituales. El cumplimiento se evalúa y se valida en un solo momento; sin embargo, depende de cada comerciante cumplir con los requisitos constantemente para garantizar una seguridad sólida. Los bancos comerciales o las marcas de pago pueden exigir ciertos requisitos para la validación formal anual del cumplimiento de la PCI DSS.
PCI DSS validada	Suministrar pruebas para garantizar el cumplimiento de todos los requisitos correspondientes de la PCI DSS en un momento determinado. Según los requisitos específicos del banco comercial o de la marca de pago, la validación puede lograrse por medio del Cuestionario de autoevaluación de la PCI DSS correspondiente o mediante un Informe sobre el cumplimiento que derive de una evaluación en el lugar.
Aplicación de pago validada por la PCI	Aplicación de software que ha sido validada por la Norma de seguridad de datos para las aplicaciones de pago (PA-DSS) de la PCI y está publicada en el sitio web del Consejo de la PCI.
Terminal de pago aprobado por la PCI	Un terminal de pago que ha sido aprobado por la norma de Seguridad de la transacción con PIN (PTS) de la PCI y está publicado en el sitio web del Consejo de la PCI.
Solución de cifrado de punto a punto publicada en la PCI	Solución de cifrado que ha sido validada por la norma de cifrado de punto a punto (P2PE) de la PCI y está publicada en el sitio web del Consejo de la PCI.
PED *	Acrónimo de "PIN entry device" (dispositivo de entrada de PIN). Teclado numérico en el cual el cliente ingresa su PIN. También denominado "PIN pad".
PIN *	Acrónimo de "personal identification number" (número de identificación personal). Número único que conoce solo el usuario y un sistema para autenticar al usuario en el sistema. Los PIN más comunes se utilizan en las transacciones de adelanto de efectivo o tarjetas con chip tipo EMV para reemplazar una firma de un titular de tarjeta. Los PIN ayudan a determinar si un titular de tarjeta está autorizado a utilizar la tarjeta e impedir su uso no autorizado si la tarjeta es robada.
Número de cuenta principal (PAN) *	Número único para tarjetas de débito y crédito que identifica la cuenta del titular de tarjeta.
Abuso de privilegio	Uso de los privilegios de acceso al sistema informático de manera abusiva. Por ejemplo cuando un administrador del sistema accede a los datos de la tarjeta con fines malintencionados o cuando alguien que roba y utiliza los privilegios de acceso elevados del administrador con fines malintencionados.
PTS *	Acrónimo de "PIN Transaction Security" de la norma de Seguridad de la transacción con PIN del Consejo de la PCI. La PTS es un conjunto de requisitos de evaluación modular para terminales de punto de interacción (POI) con aceptación de PIN. Consulte los detalles en www.pcisecuritystandards.org.
QIR *	Acrónimo de "Qualified Integrator or Reseller" (integrador o revendedor certificado). Consulte los detalles en *www.pcisecuritystandards.org*.

Glosario

TÉRMINO	DEFINICIÓN
Evaluador de Seguridad Certificado (QSA) *	Una compañía aprobada por el PCI Security Standards Council para validar que una entidad cumple con los requisitos de la PCI DSS.
Pago recurrente	Un método de facturación que los comerciantes utilizan para cobrarles a sus clientes reiteradamente de forma continuada en el tiempo, como en casos de suscripciones o membresías mensuales. Una forma segura de hacer esto es que el adquirente/procesador realice una tokenización de los datos de la tarjeta, lo cual garantiza su protección y exime al comerciante de su responsabilidad.
Acceso remoto *	Acceso a una red informática desde una ubicación externa a esa red. Las conexiones de acceso remoto pueden originarse tanto desde la propia red de la empresa como desde una ubicación remota. Una red privada virtual (VPN) es un ejemplo de tecnología de acceso remoto. El acceso remoto puede ser interno (p. ej.: soporte de TI) o externo (p. ej.: proveedores de servicios, agentes externos, integradores/revendedores).
Revendedor / integrador *	Una entidad que vende y/o integra aplicaciones de pago, pero no las desarrolla.
Router *	Hardware o software que conecta dos o más redes informáticas internas o externas para "dirigir" u orientar datos a través de una red y asegurarse de que los datos se transfieren correctamente entre esas redes. Además, el router puede ofrecer mayor seguridad, dado que solo permite el tráfico aprobado y bloquea el tráfico no aprobado.
Lector de tarjetas seguro (SCR)	Un dispositivo aprobado por la PTS que se conecta a un teléfono móvil o tableta para aceptar de forma segura tarjetas de pago. Los SCR aprobados por la PTS de la PCI protegen y cifran los datos de la tarjeta a través del SRED. Consulte también *SRED*.
Código de seguridad *	Un valor de tres o cuatro dígitos impreso en el anverso o reverso del panel de firma de una tarjeta de pago. Este código está asociado exclusivamente a una sola tarjeta y se utiliza como una verificación adicional para garantizar que la tarjeta esté en posesión del titular de tarjeta legítimo, generalmente durante una transacción de tarjeta ausente. También denominado código de seguridad de la tarjeta.
Cuestionario de autoevaluación (SAQ) *	Herramienta de validación de la PCI DSS que documenta resultados de autoevaluación de la evaluación de la PCI DSS realizada por una entidad.
Datos confidenciales de autenticación *	Información relacionada con la seguridad que se utiliza para autenticar a los titulares de tarjeta y/o autorizar transacciones de tarjetas de pago que se almacenan en el chip o en la banda magnética de la tarjeta.
Proveedor de servicios *	Una entidad comercial que ofrece distintos servicios a los comerciantes. Generalmente, estas entidades almacenan, procesan o transmiten datos de la tarjeta en nombre de otra entidad (como un comerciante) O son proveedores de servicios administrados que ofrecen firewalls administrados, detección de intrusiones, hosting y otros servicios relacionados con TI. También denominado "proveedor".
Duplicación	Robar datos de la tarjeta directamente de la tarjeta de pago del consumidor o desde una infraestructura de pago en la tienda del comerciante, como un lector de tarjetas portátil peligroso o a través de modificaciones realizadas al terminal de pago del comerciante. El objetivo es cometer un fraude, la amenaza es grave, y puede suceder en cualquier entorno del comerciante.

Glosario

TÉRMINO	DEFINICIÓN
Dispositivo de duplicación	Un dispositivo físico que suele estar unido a un dispositivo para lectura de tarjetas legítimo, y cuya finalidad es captar o almacenar (o ambas cosas) en forma ilegal la información de una tarjeta de pago. También denominado "dispositivo de robo de tarjeta".
Pequeño comerciante	Una empresa que generalmente cuenta con una sola tienda o posiblemente algunas sucursales, con un presupuesto muy limitado a nulo para TI y con frecuencia no cuenta con personal de TI.
SRED	Acrónimo de "secure reading and exchange of data" (intercambio y lectura de datos seguros). Un conjunto de requisitos de PTS de la PCI diseñado para proteger y cifrar los datos de la tarjeta en terminales de pago. Una solución de cifrado de punto a punto (P2PE) publicada en el sitio del PCI Council debe utilizar un terminal de pago publicado y aprobado por PTS habilitado con SRED y que realice activamente el cifrado de los datos de la tarjeta.
Terminal independiente	Un terminal de pago que no depende de ninguna conexión a otro dispositivo dentro del entorno del comerciante y no realiza otras funciones. El único requisito para funcionar es una conexión al procesador a través de una conexión a Internet o una línea telefónica. Si el terminal requiere conexión a una caja registradora electrónica computarizada o tiene varias funciones (como un dispositivo móvil), no es un terminal independiente.
Autenticación segura	Se utiliza para verificar la identidad de un usuario o dispositivo a fin de resguardar la seguridad del sistema que protege. El término autenticación segura generalmente es sinónimo de autenticación de múltiples factores (MFA).
Till	Consulte *Caja registradora electrónica*.
Tokenización	Un proceso por el cual el número de cuenta principal (PAN) se reemplaza por un valor sustituto denominado token. Los tokens pueden utilizarse en lugar del PAN original para realizar funciones cuando la tarjeta está ausente como anulaciones, reintegros o facturación recurrente. Además, los tokens ofrecen mayor seguridad si fuera robado porque es información inutilizable y además no tiene ningún valor para los delincuentes.
Datos no cifrados	Cualquier dato que se pueda leer sin la necesidad de descifrarlo primero. También denominados datos de "texto simple" y "texto claro".
Proveedor	Una entidad comercial que le provee a un comerciante de un producto o servicio necesario para el desarrollo de actividades comerciales. Cuando se ofrecen servicios, el proveedor puede considerarse un proveedor de servicios y puede requerir el acceso a las ubicaciones físicas o sistemas informáticos dentro del entorno del comerciante, lo que podría afectar la seguridad de los datos de la tarjeta. También consulte *Proveedor de servicios*.
Terminal de pago virtual *	Acceso basado en el navegador web al sitio web de un adquirente, procesador o proveedor de servicios externo para autorizar las transacciones de una tarjeta de pago. A diferencia de los terminales físicos, los terminales de pago virtuales no leen datos directamente de una tarjeta de pago. El comerciante ingresa los datos de la tarjeta de pago de forma manual a través del navegador web conectado de forma segura. Debido a que las transacciones de tarjetas de pago se ingresan manualmente, comúnmente se utilizan terminales de pago virtuales en lugar de terminales físicos en entornos de comerciantes con bajo volumen de transacciones.

Glosario

Red Privada Virtual (VPN) *	La VPN está compuesta de circuitos virtuales dentro de una rede más amplia, como Internet, en lugar de conexiones directas por medio de cables físicos. Los extremos de la VPN "atraviesan" una red más amplia, lo que se hace para crear una conexión privada y segura.
Virus	Malware que duplica las copias de sí mismo en otro software o archivos de datos en una computadora "infectada". Una vez realizada la duplicación, el virus puede ejecutar una carga útil maliciosa, como borrar todos los datos de la computadora. Un virus puede permanecer inactivo y ejecutar su carga útil posteriormente, o quizá nunca desencadene una acción maliciosa. Un virus que se duplica y se reenvía a sí mismo como un adjunto de correo electrónico o como parte de un mensaje de la red se denomina "gusano".
Vulnerabilidad *	Error o debilidad que, de llegar a explotarse, puede ocasionar una exposición a riesgos del sistema, intencionalmente o no.
Análisis de vulnerabilidades	Una herramienta de software que detecta y clasifica posibles puntos débiles (vulnerabilidades) de una computadora o red. Un análisis puede ser realizado por el departamento de TI de la organización o por un proveedor de servicios de seguridad (como un Proveedor aprobado de escaneo). Consulte también *Proveedor aprobado de escaneo (ASV)*.
Wi-Fi *	Red inalámbrica que conecta computadoras sin necesidad de una conexión física de cables.
Terminal de pago inalámbrico	Un terminal de pago que se conecta a Internet utilizando una de las distintas tecnologías inalámbricas.