Glosario de términos de seguridad de pagos y de la información

PRINCIPIOS BÁSICOS DE SEGURIDAD DE DATOS PARA PEQUEÑOS COMERCIANTES
UN PRODUCTO DEL GRUPO DE TRABAJO DE PEQUEÑOS COMERCIANTES DE LA INDUSTRIA DE TARJETAS DE PAGO

VERSIÓN 2.0 | AGOSTO DE 2018

PCI Security Standards Council®

Introducción

Este *Glosario de términos de seguridad de pagos y de la información es* un complemento de la sección de *Guía de pagos seguros,* parte de los Principios básicos de seguridad de datos para pequeños comerciantes. Su propósito es explicar los términos pertinentes sobre seguridad de la información y la Industria de tarjetas de pago (PCI) en un lenguaje sencillo.

Las definiciones de términos marcados con un asterisco (*) se basan o derivan de *las definiciones de la Norma de seguridad de datos (DSS) de la Industria de tarjetas de pago (PCI) y la Norma de seguridad de datos de aplicaciones de pago (PA-DSS): Glosario de términos, abreviaturas y acrónimos. Se considera que la última versión de este glosario es la* fuente autorizada, y deben consultarse en ella las definiciones actuales y completas de PCI DSS y PA-DSS.

Consulte los Principios básicos de seguridad de datos para pequeños comerciantes en los siguientes casos:

RECURSO	URL
Guía para realizar pagos seguros	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf*
Sistemas de pago comunes	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Preguntas para sus proveedores	*https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf*
Herramienta de evaluación	*http://www.pcisecuritystandards.org/merchants/ds.org/merchants/* Esta herramienta se proporciona únicamente a título informativo para los comerciantes. Una opción para los comerciantes es usarla como primer paso para informarse sobre las prácticas de seguridad pertinentes con respecto a la forma en que aceptan pagos, proporcionar sus respuestas iniciales y ver los resultados.

Glosario

TÉRMINO	DEFINICIÓN
Abuso de privilegios	Abuso de los privilegios de acceso al sistema informático. Por ejemplo, un administrador de sistemas que accede a los datos de una tarjeta o alguien que roba y utiliza los elevados privilegios de acceso de un administrador con malas intenciones.
Acceso remoto *	Acceso a una red informática desde una ubicación externa. Las conexiones de acceso remoto pueden originarse desde la propia red de la empresa o desde una ubicación remota. Un ejemplo de tecnología de acceso remoto es una red privada virtual (VPN). El acceso remoto puede ser interno (por ejemplo, soporte de TI) o externo (tales como proveedores de servicios, agentes de terceros, integradores/revendedores).
Aceptación de pago por medio de dispositivo móvil	Uso de un dispositivo móvil para aceptar y procesar las transacciones de pago. El dispositivo móvil normalmente viene con un accesorio de lector de tarjetas disponible en el mercado
Adquirente *	Ver *Banco mercantil* y Procesador de pagos.
Análisis de vulnerabilidad	Herramienta de software que detecta y clasifica los posibles puntos débiles (vulnerabilidades) de una computadora o red. El análisis trimestral de vulnerabilidad externa según el requisito 11.2.2 de la PCI DSS debe realizarlo un proveedor de servicios de análisis. Otros análisis de vulnerabilidad (como los internos y los realizados después de cambios en la red) pueden estar a cargo de personal certificado del departamento de TI de una organización o por un proveedor de servicios de seguridad (como un proveedor aprobado de análisis). *Véase también Proveedor aprobado de análisis (ASV)*.
Aplicación *	Programa de software o grupo de programas que se ejecutan en una PC, smartphone, tablet, servidor interno o servidor web.
Aplicación de pago *	En relación 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 las transacciones de pago.
Aplicación de pago validada conforme a la PCI	Aplicación de software que ha sido validada según la norma de seguridad de datos de aplicaciones de pago de PCI (PA-DSS) y que aparece en el sitio web de PCI Council.
Asesor de seguridad certificado (QSA)*	Empresa aprobada por PCI Security Standards Council para validar la adherencia de una entidad a los requisitos de la PCI DSS.
Ataque cibernético	Cualquier acción ofensiva para irrumpir en una computadora o sistema. Los ataques cibernéticos pueden ir desde la instalación de spyware en una PC, la irrupción en un sistema de pago para robar datos de tarjetas o el intento de destruir la infraestructura esencial, como la red eléctrica.
Autenticación *	Método para verificar la identidad de una persona, dispositivo o proceso que intenta acceder a una computadora. Para confirmar la validez de la identidad o usuario, se proporcionan uno o más de los siguientes datos: • Contraseña o frase de seguridad (algo que el usuario conoce) • Token, tarjeta inteligente o certificado digital único para el usuario (algo que el usuario tiene) • Un identificador biométrico, como una huella dactilar (algo inherente al usuario o a lo que hace)

Glosario

TÉRMINO	DEFINICIÓN
Autenticación multifactorial *	Método de autenticación de un usuario cuando se verifican dos o más factores. Estos factores incluyen algo que el usuario tiene (como una tarjeta inteligente o una llave electrónica), algo que el usuario conoce (como una contraseña, una frase de seguridad o un PIN) o algo inherente al usuario o a lo que hace (como huellas dactilares, otras formas de autenticación biométrica, etc.).
Autenticación sólida	Se utiliza para verificar la identidad de un usuario o dispositivo para garantizar la seguridad del sistema que protege. El término "autenticación sólida" a menudo significa con autenticación multifactorial (MFA).
Autorización *	En una transacción con tarjeta de pago, la autorización se produce cuando el comerciante recibe la aprobación de la transacción después de que el adquirente la valida con el emisor/procesador.
Banco del comerciante *	Banco o institución financiera que procesa pagos con tarjeta de crédito y/o débito en nombre de los comerciantes. También llamado "adquirente", "banco adquirente", "procesador de tarjeta" o "procesador de pago". Véase también Procesador de pago.
Caja registradora	Véase *Caja registradora electrónica*.
Chip	También conocido como "chip tipo EMV". El microprocesador (o "chip") de una tarjeta de pago que se utiliza al procesar las transacciones de acuerdo con las especificaciones internacionales para las transacciones tipo EMV.
Chip y firma	Proceso de verificación en el que el consumidor utiliza su firma con una terminal de pago habilitada para chip tipo EMV al comprar bienes o servicios.
Chip y PIN	Proceso de verificación en el que el consumidor introduce su PIN en una terminal de pago habilitada con chip tipo EMV al comprar bienes o servicios.
Cifrado	Proceso de uso de la criptografía para convertir matemáticamente la información en un formato inutilizable excepto para los titulares de una clave digital específica. El uso del cifrado protege la información devaluándola ante los delincuentes. Véase también *Criptografía*.
Código de seguridad *	Valor de tres o cuatro dígitos impreso en el panel de firma frontal o posterior de una tarjeta de pago. Este código está asociado exclusivamente a una tarjeta individual y se utiliza como revisión adicional para garantizar que la tarjeta esté en posesión del titular legítimo, generalmente durante una transacción en la que no se presenta la tarjeta. También se conoce como código de seguridad de la tarjeta.
Contraseña *	Palabra, frase o cadena de caracteres para autenticar a un usuario. Al combinarse con el nombre del usuario, la contraseña tiene como objetivo comprobar la identidad del usuario para acceder a los recursos informáticos.
Contraseña predeterminada	Contraseña simple que viene con un nuevo software o hardware. Una contraseña predeterminada (como "admin", "contraseña" o "123456") es fácil de adivinar y suele estar disponible en línea. Está prevista como un marcador de posición y no ofrece ninguna seguridad real: debe cambiarse por una contraseña más segura después de instalarse un nuevo software o hardware.

Glosario

TÉRMINO	DEFINICIÓN
Credencial	Información utilizada para identificar y autenticar al usuario para acceder a un sistema. Por ejemplo, las credenciales suelen ser el nombre de usuario y la contraseña. Pueden incluir huella dactilar, lector de retina o un número único que se obtiene a partir de un "generador de token" portátil. La seguridad es mayor cuando el acceso requiere múltiples credenciales.
Criptografía	La criptografía es el método para asegurar los datos haciéndolos ininteligibles para el ser humano o una computadora. La criptografía solo es útil cuando el destinatario previsto puede reagrupar los datos en un formato legible utilizando un método que solo conocen el emisor y el receptor. Véase también *Cifrado*.
Cuestionario de autoevaluación (SAQ)	Cuestionario que abarca un conjunto de requisitos de la PCI DSS y que lo contesta la propia organización para confirmar que cumple con dichos requisitos.
Cumplimiento con PCI DSS	Cumplir con todos los requisitos aplicables de la PCI DSS, con un enfoque de continuidad de los procesos habituales. El cumplimiento se evalúa y valida en un solo momento; sin embargo, depende de cada comerciante seguir los requisitos de forma continua para proporcionar una seguridad sólida. Los bancos comerciales y/o las marcas de pago pueden tener requisitos para la validación anual formal del cumplimiento de la PCI DSS.
Datos confidenciales de autenticación *	Información relacionada con la seguridad que se utiliza para autenticar a los titulares de las tarjetas y/o autorizar las transacciones de las tarjetas de pago, almacenada en la banda magnética o el chip de la tarjeta.
Datos de la tarjeta/Datos de la tarjeta del cliente *	Como mínimo, los datos de la tarjeta incluyen el número de cuenta principal (PAN) y también pueden incluir el nombre del titular de la tarjeta y la fecha de vencimiento. El PAN está visible en la parte delantera de la tarjeta y se codifica en la banda magnética y/o en el chip integrado. También se conocen como datos del titular de la tarjeta. Consulte también *Datos confidenciales de autenticación* para ver elementos de datos adicionales que pueden ser parte de una transacción de pago, pero que no deben almacenarse después de que se haya autorizado la transacción.
Datos no encriptados	Cualquier dato que sea legible sin la necesidad de descifrarlo primero. También llamados datos de "texto simple/plano".
Dispositivo de skimming	Dispositivo físico, a menudo conectado a un dispositivo de lectura de tarjetas, diseñado para capturar y/o almacenar ilegalmente la información de una tarjeta de pago. También llamado "dispositivo de robo de tarjetas".
Dispositivo móvil	Dispositivos, como smartphones y tablets, pequeños y portátiles que pueden conectarse a redes informáticas de forma inalámbrica.
Firewall *	Hardware y/o software que protege los recursos de la red contra accesos no autorizados. Un firewall permite o rechaza la comunicación entre equipos o redes con diferentes niveles de seguridad en función de un conjunto de reglas y otros criterios.
Hacker	Persona u organización que intenta eludir las medidas de seguridad de los sistemas informáticos para obtener control y acceso. Por lo general, esto se hace con el objetivo de robar datos de tarjetas.
Integrador/Revendedor	Un integrador/revendedor es una empresa con la que trabajan los comerciantes para ayudar a establecer su sistema de pago. Esto puede incluir la instalación, configuración y soporte. Estas empresas también pueden vender los dispositivos o aplicaciones de pago como parte de su servicio. Véase también Integrador o revendedor certificado (QIR).

Glosario

TÉRMINO	DEFINICIÓN
Investigador forense	Los investigadores forenses de PCI (PFI) son empresas aprobadas por PCI Council para ayudar a determinar cuándo y cómo se vulneraron los datos de una tarjeta. Realizan investigaciones dentro de la industria financiera utilizando metodologías y herramientas de investigación comprobadas. También colaboran en la aplicación estricta de la ley apoyando a los interesados con las investigaciones de delitos resultantes.
Lector de tarjetas seguro (SCR)	Dispositivo aprobado por PTS que se conecta a un teléfono móvil o tablet para aceptar tarjetas de pago de forma segura. El SCR aprobado por el PTS de la PCI protege y cifra los datos de la tarjeta a través de SRED. Véase también SRED.
Lo que el negocio necesita saber	El principio de que el acceso a los sistemas o a los datos se otorga por necesidad comercial del usuario: solo lo necesario para su función de trabajo.
Malware *	Software malicioso diseñado para infiltrarse en un sistema informático con la intención de robar datos, o dañar aplicaciones o el sistema operativo. Este software normalmente ingresa a la red durante actividades comerciales aprobadas, como al usar un correo electrónico o navegar en sitios web. Algunos ejemplos de malware incluyen virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.
Máquina registradora electrónica (ECR)	Dispositivo que registra y calcula transacciones y puede imprimir recibos, pero no acepta pagos con tarjeta del cliente. También se le denomina “caja registradora”.
Middleware de pago	Término general para el software que conecta dos o más aplicaciones de pago, probablemente no relacionadas. Por ejemplo, puede pasar datos de tarjetas entre una aplicación en una terminal de pago y otros sistemas del comerciante que envían datos de las tarjetas a un procesador.
Número de cuenta principal (PAN)	Número único para tarjetas de crédito y débito que identifica la cuenta del titular de la tarjeta.
Número de identificación bancaria (BIN)	Primeros seis dígitos (o más) de un número de tarjeta de pago que identifica a la institución financiera que emitió la tarjeta de pago al titular.
P2PE	Acrónimo de la norma de cifrado de punto a punto de PCI Security Standards Council. Véase más detalles en *www.pcisecuritystandards.org*
PA-DSS *	Acrónimo de la norma de seguridad de datos de la aplicación de pago de PCI Security Standards Council. Véase más detalles en *www.pcisecuritystandards.org*
Pago recurrente	Método de facturación en el que los comerciantes facturan a sus clientes en repetidas ocasiones, como las suscripciones o membresías mensuales. Una forma segura de hacerlo es que el adquirente/procesador aplique un token en los datos de la tarjeta, lo cual garantiza su protección y libera al comerciante de esta responsabilidad.
Parche *	Actualización del software que agrega funcionalidad o corrige un defecto (o “error”).

Glosario

TÉRMINO	DEFINICIÓN
PCI *	Acrónimo de “Industria de tarjetas de pago”.
PCI DSS *	Acrónimo de la norma de seguridad de datos de la Industria de tarjetas de pago de PCI Council. Véase más detalles en *www.pcisecuritystandards.org*
PED *	Acrónimo de “dispositivo de entrada de PIN”. Teclado en el que el cliente ingresa su PIN. También se denomina “ensamblador de PIN”.
Pequeño comerciante	Un pequeño comerciante suele ser un negocio de propiedad y gestión independientes con una o varias ubicaciones, y con un presupuesto de TI limitado o nulo y, a menudo, sin personal de TI. La marca de pago o el adquirente (banco del comerciante) determina si se requiere que el pequeño comerciante valide el cumplimiento con la PCI.
PIN *	Acrónimo de “número de identificación personal”. Un número único conocido solo por el usuario y un sistema para autenticar al usuario en el sistema. Los PIN típicos se utilizan en cajeros automáticos para transacciones de disposición de efectivo o tarjetas con chip tipo EMV para reemplazar la firma del titular de la tarjeta. Los PIN ayudan a determinar si el titular de la tarjeta está autorizado a utilizarla y a impedir su uso no autorizado en caso de robo de la tarjeta.
Principios básicos de seguridad de datos (DSE)	Los principios básicos de seguridad de datos para pequeños comerciantes representan un conjunto de recursos educativos y una herramienta de evaluación para ayudar a los comerciantes a simplificar su seguridad y reducir riesgos. Los DSE se conciben como una propuesta alterna a los cuestionarios de autoevaluación (SAQ) de la DSS PCI para aquellos comerciantes designados como elegibles por las marcas de pago y sus adquirentes (bancos del comerciante).
Procesador de pago *	Entidad contratada por los comerciantes para manejar las transacciones con tarjeta de pago en su nombre. Si bien los procesadores de pago suelen proporcionar servicios de compra, los procesadores de pago no se consideran adquirentes (bancos del comerciante) a menos que una marca de tarjeta de pago los defina como tal. También se denominan “puerta de enlace de pago” o “proveedor de servicios de pago” (PSP). Véase también *Banco del comerciante*”.
Proveedor aprobado de análisis (ASV) *	Empresa aprobada por el PCI Security Standards Council para llevar a cabo servicios de análisis de vulnerabilidades externas para identificar las debilidades comunes en la configuración del sistema.
Proveedor de hosting *	Ofrece varios servicios a comerciantes y otros proveedores de servicios, donde los datos de los clientes están “alojados” o se encuentran dentro de los servidores del proveedor. Los servicios típicos incluyen espacio compartido para múltiples comerciantes en un servidor, un servidor exclusivo para un comerciante o aplicaciones web, como un sitio web con opciones de “carrito de compras”.
Proveedor de la aplicación de pago	Proveedor que vende aplicaciones que almacenan, procesan y/o transmiten datos de tarjetas durante las transacciones de pago.

Glosario

TÉRMINO	DEFINICIÓN
Proveedor de servicios *	Entidad comercial que proporciona varios servicios a los comerciantes. Por lo general, estas entidades almacenan, procesan o transmiten datos de tarjetas en nombre de otra entidad (como un comerciante) o bien, son proveedores de servicios gestionados que proporcionan firewalls, detección de intrusiones, hosting y otros servicios relacionados con TI. También llamado “suministrador”.
Proveedor del sistema de pago	Proveedor que vende, otorga licencias o distribuye una solución de pago completa a un comerciante. La solución comprende el hardware y software necesarios para manejar los pagos dentro de la tienda, y proporciona un método para conectarse a un procesador de pago.
PTS *	Acrónimo de la norma de seguridad de transacciones con PIN de PCI Council. PTS es un conjunto de requisitos de evaluación modular para las terminales de puntos de interacción (POI) de aceptación de PIN. Véase más detalles en *www.pcisecuritystandards.org*
QIR *	Acrónimo de “integrador o revendedor certificado”. Los QIR son integradores y revendedores especialmente capacitados por PCI Security Standards Council para abordar controles de seguridad críticos al instalar los sistemas de pago de los comerciantes. Véase más detalles en *www.pcisecuritystandards.org*
Red *	Dos o más computadoras conectadas por medios físicos o inalámbricos.
Red privada virtual (VPN)*	Software que crea un canal seguro y privado para intercambiar datos y realizar llamadas telefónicas a través de internet.
Registro *	Archivos que se crean automáticamente cuando se presentan ciertas situaciones predefinidas (a menudo, relacionadas con seguridad) dentro de una red o sistema informático. Los datos del registro incluyen el sello de fecha y hora, la descripción de la situación y la información exclusiva de esa situación. Estos archivos son útiles para la resolución de problemas técnicos o en una investigación de vulnerabilidad de datos. También llamado “registro de auditoría” o “pista de auditoría”.
Revendedor/Integrador *	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 “enrutar” o guiar los datos a través de una red, y para garantizar que los datos fluyan correctamente entre esas redes. El router también puede crear más seguridad al permitir solo el tráfico aprobado y rechazar el tráfico no aprobado.
Sistema de pago	Comprende todo el proceso de aceptación de pagos con tarjeta en un establecimiento comercial minorista (como tiendas o comercios o escaparates de comercio electrónico) y puede incluir una terminal de pago, una caja registradora electrónica, otros dispositivos o sistemas conectados a la terminal de pago (por ejemplo, wifi para la conectividad o una PC para el inventario), servidores con componentes de comercio electrónico como páginas de pago, y conexiones con el banco del comerciante.
Sistema operativo *	Software de un sistema informático que permite la gestión y coordinación general de las actividades informáticas. Algunos ejemplos: Microsoft Windows, Apple OSX, iOS, Android, Linux y UNIX.

Glosario

TÉRMINO	DEFINICIÓN
Skimming	Robo de datos de tarjetas directamente de la tarjeta de pago del consumidor o desde la infraestructura de pago en la ubicación del comerciante, como con un lector de tarjetas portátil no autorizado o mediante modificaciones realizadas a la terminal de pago del comerciante. Su propósito es cometer fraude, la amenaza es grave y puede afectar el entorno de cualquier comerciante.
Software antivirus *	Programa de software que detecta, elimina y protege contra software malicioso (también llamado "malware"), incluyendo virus, gusanos, troyanos o caballos de Troya, spyware, adware y rootkits. También llamado "software anti-malware".
Solución de cifrado de punto a punto conforme a la PCI	Solución de cifrado que ha sido validada según la norma de cifrado de punto a punto de PCI (P2PE) y que figura en el sitio web de PCI Council.
SRED	Acrónimo de "Lectura e intercambio seguros de datos". Conjunto de requisitos de PTS de la PCI diseñados para proteger y codificar los datos de las tarjetas en las terminales de pago. La solución de cifrado de punto a punto (P2PE) conforme a PCI Council debe utilizar una terminal de pago aprobada y considerada por PTS habilitada con SRED, y realizar activamente el cifrado de datos de la tarjeta.
Suministrador	Entidad comercial que suministra a un comerciante un producto o servicio necesario para el negocio. Cuando se ofrecen servicios, el suministrador puede considerarse un proveedor de servicios y requerir acceso a ubicaciones físicas o sistemas informáticos dentro del entorno del comerciante que podrían afectar la seguridad de los datos de las tarjetas. Véase también *Proveedor de servicios*.
Terminal autónoma	Terminal de pago que no depende de la conexión a ningún otro dispositivo dentro del entorno del comerciante y no realiza ninguna otra función. El único requisito para que funcione es una conexión con el procesador a través de una conexión a internet o de una línea telefónica. Si la terminal requiere conexión a una caja registradora electrónica computarizada o tiene múltiples funciones (como un dispositivo móvil), no es una terminal independiente.
Terminal de pago	Dispositivo de hardware utilizado para aceptar pagos al deslizar, introducir, insertar o tocar la tarjeta del cliente. También se denomina "terminal de punto de venta (POS)", "máquina de tarjeta de crédito" o "terminal PDQ".
Terminal de pago aprobada por la PCI	Terminal de pago que ha sido aprobada conforme a la norma de seguridad de transacciones con PIN (PTS) de la PCI y que aparece en el sitio web de PCI Council.
Terminal de pago inalámbrica	Terminal de pago que se conecta a internet utilizando cualquiera de las diversas tecnologías inalámbricas.
Terminal de pago integrada	Una terminal de pagos y una caja registradora electrónica en un dispositivo que recibe pagos, registra y calcula las transacciones e imprime recibos.

Glosario

TÉRMINO	DEFINICIÓN
Terminal de pago virtual *	Acceso con base en un navegador web al sitio web de un adquirente, procesador o sitio web de un tercero proveedor de servicios para autorizar transacciones con tarjeta de pago. A diferencia de las terminales físicas, las terminales de pago virtuales no leen los datos directamente de una tarjeta de pago. El comerciante registra de forma manual los datos de la tarjeta de pago a través del navegador web conectado de forma segura. Dado que las transacciones con tarjeta de pago se registran de forma manual, las terminales de pago virtual se suelen utilizar en lugar de terminales físicas en entornos del comerciante con bajos volúmenes de transacciones.
Tokenización	Proceso por el cual el número de cuenta principal (PAN) se sustituye por un valor alterno llamado token. Los tokens se pueden utilizar en lugar del PAN original para realizar funciones cuando la tarjeta está ausente, como anulaciones, reembolsos o facturación recurrente. También proporcionan mayor seguridad si se los roban porque no se pueden usar y, por lo tanto, no tienen valor para un delincuente.
Validación conforme a la PCI DSS	Proporcionar una prueba de que todos los requisitos aplicables de la PCI DSS se cumplen en un solo momento. Dependiendo de los requisitos específicos del banco comercial y/o de la marca de pago, la validación puede lograrse mediante el cuestionario de autoevaluación de la PCI DSS aplicable o mediante un Informe de cumplimiento resultante de una evaluación in situ.
Virus	Malware que replica copias de sí mismo en otro software o archivos de datos en un equipo “infectado”. Al replicarse, el virus puede ejecutar una carga maliciosa, como borrar todos los datos de la computadora. Un virus puede permanecer inactivo y ejecutar su carga más tarde o puede que nunca desencadene una acción maliciosa. Un virus que se replica a sí mismo al reenviarse como un archivo adjunto de un correo electrónico o como parte de un mensaje de red se denomina “gusano”.
Vulnerabilidad *	Falla o debilidad que, si se abusa de ella, puede dar como resultado poner en riesgo, de forma intencional o no intencional, un sistema.
Vulnerabilidad de datos	La vulnerabilidad de datos es un incidente en el que un tercero no autorizado posiblemente pudo ver, robar o utilizar datos confidenciales. Puede involucrar datos de tarjetas, información de salud personal (PHI), información de identificación personal (PII), secretos comerciales, propiedad intelectual, etc.
Wifi*	Red inalámbrica que conecta equipos sin una conexión física con cables.