Industria de Tarjetas de Pago (PCI)
Normas de Seguridad de Datos (DSS) y Aplicación de pago Norma de seguridad de datos (PA-DSS)

Glosario de términos, abreviaturas y acrónimos

Versión 3.2

Abril de 2016

Término	Definición
AAA	Acrónimo de “authentication, authorization, and accounting” (autenticación, autorización y contabilización). Protocolo para autenticar a un usuario basándose en la identidad verificable del usuario, autorizar a un usuario basándose en sus derechos de usuario y contabilizar el consumo de recursos de una red de un usuario.
Control de acceso	Mecanismo que limita la disponibilidad de información o de los recursos necesarios para su procesamiento sólo a personas o aplicaciones autorizadas.
Datos de cuentas	Los datos de cuentas constan de los datos de titulares de tarjetas o los datos confidenciales de autenticación. Consulte *Datos de titulares de tarjetas* y *Datos confidenciales de autenticación.*
Número de cuenta	Consulte *Número de cuenta principal (PAN).*
Adquirente	También denominado “banco comercial”, “banco adquirente” o “institución financiera adquirente”. Entidad, por lo general una institución financiera, que procesa transacciones con tarjetas de pago para comerciantes y está definida por una marca de pago como un adquiriente. Los adquirientes están sujetos a los reglamentos de las marcas de pago y a los procedimientos relacionados con el cumplimiento por parte del comerciante. Ver también *Procesador de pago.*
Acceso administrativo	Privilegios elevados o aumentados que se otorgan a una cuenta para que ésta administre sistemas, redes y/o aplicaciones. Es posible asignar acceso administrativo a la cuenta de una persona o a una cuenta de sistemas integrada. Las cuentas con acceso administrativo también se conocen como “superusuario”, “root”, “administrador”, “admin”, “sysadmin” o “estado de supervisor”, dependiendo del sistema operativo particular y la estructura organizativa.
Adware	Tipo de software malicioso cuya instalación hace que la computadora muestre o descargue publicidad de manera automática.
AES	Abreviatura de “Advanced Encryption Standard” (norma de cifrado avanzado). Cifrado por bloques utilizado en la criptografía de clave simétrica que adoptó el NIST en noviembre de 2001 como U.S. FIPS PUB 197 (o “FIPS 197”). Consulte *Criptografía sólida.*
ANSI	Acrónimo de “American National Standards Institute” (Instituto Estadounidense de Normas). Organización privada y sin fines de lucro que administra y coordina el sistema de evaluación de conformidad y normalización voluntaria de los Estados Unidos.
Antivirus	Programa o software capaz de detectar y eliminar los diferentes tipos de programas maliciosos (también conocidos como "malware"), incluidos virus, gusanos, troyanos o caballos troyanos, spyware, adware y rootkits, y de proteger su computadora contra estos.
AOC	Acrónimo de “attestation of compliance” (atestación de cumplimiento). La declaración de cumplimiento es un formulario para los comerciantes y proveedores de servicios que permite declarar respecto de los resultados de una evaluación de las PCI DSS, según está documentado en el Cuestionario de autoevaluación o Informe de cumplimiento.

Término	Definición
AOV	Acrónimo de “attestation of validation” (declaración de validación). La declaración de validación es un formulario para los PA-QSA que permite declarar respecto de los resultados de una evaluación de las PA-DSS, según está documentado en el Informe de validación de PA-DSS.
Aplicación	Incluye todos los programas o grupos de programas de software adquiridos y personalizados, así como también las aplicaciones internas y externas (por ejemplo, aplicaciones web).
ASV	Acrónimo de “Approved Scanning Vendor” (proveedor aprobado de análisis). Empresa aprobada por el SSC de la PCI para prestar servicios de análisis de vulnerabilidades externas.
Registro de auditoría	También denominado “pista de auditoría”. Registro cronológico de las actividades del sistema. Esta herramienta proporciona una pista independientemente verificable que permite la reconstrucción, revisión y evaluación de la secuencia de entornos y actividades que rodean o conducen a las operaciones, los procedimientos o eventos relacionados a una transacción desde el inicio hasta los resultados finales.
Pista de auditoría	Consulte *Registro de auditoría.*
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 el usuario sepa, como una contraseña o frase de seguridad ▪ Algo que el usuario tenga, como un dispositivo token o una tarjeta inteligente ▪ Algo que el usuario sea, como un rasgo biométrico
Credenciales de autenticación	Combinación del ID de usuario o ID de la cuenta más el (los) factor(es) utilizado(s) para autenticar a un individuo, dispositivo o proceso,
Autorización	En el contexto del control de acceso, la autorización es el otorgamiento de derechos de acceso u otros derechos similares a un usuario, programa o proceso. La autorización define lo que un individuo o programa puede hacer después de un proceso de autenticación satisfactorio. En lo que se refiere a una transacción con tarjeta de pago, la autorización ocurre cuando un comerciante recibe la aprobación de la transacción después de que el adquirente valide la transacción con el emisor/procesador.
Copia de seguridad	Copia duplicada de datos que se realiza con el fin de archivarla o protegerla de daños o pérdidas.
BAU	Acrónimo de “business as usual” (procesos habituales). BAU implica las operaciones comunes diarias comerciales de una organización.
Bluetooth	Protocolo inalámbrico que utiliza tecnología de comunicación de corto alcance y permite la transmisión de datos entre dos dispositivos ubicados a poca distancia.

Término	Definición
Desbordamiento de buffer	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y en el que un programa desborda el límite del buffer y escribe datos en el espacio de memoria adyacente. Los desbordamientos de buffer son aprovechados por los atacantes para obtener acceso no autorizado a los sistemas o datos.
Dispositivo de robo de tarjeta	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.
Código o valor de verificación de la tarjeta	También denominado Código o valor de validación de la tarjeta o Código de seguridad de la tarjeta. Se refiere a: (1) datos de banda magnética o (2) funciones de seguridad impresas. (1) Elementos de datos en la banda magnética de una tarjeta que utilizan procesos criptográficos seguros para proteger la integridad de los datos de la banda y evidencia cualquier alteración o falsificación. Conocida como CAV, CVC, CVV o CSC, según la marca de la tarjeta de pago. La siguiente lista especifica los términos según la marca de la tarjeta: ▪ **CAV –** Card Authentication Value (valor de autenticación de la tarjeta) (tarjetas de pago JCB) ▪ **PAN CVC –** Card Validation Code (código de validación de la tarjeta) (tarjetas de pago MasterCard) ▪ **CVV –** Card Verification Value (valor de verificación de la tarjeta) (tarjetas de pago Visa y Discover) ▪ **CSC –** Card Security Code (código de seguridad de la tarjeta) (tarjetas de pago American Express (2) En el caso de las tarjetas de pago Discover, JCB, MasterCard y Visa, el segundo tipo de valor o código de validación de la tarjeta es el valor de tres dígitos impreso que se encuentra más a la derecha de la zona del panel de firma, en el reverso de la tarjeta. En el caso de las tarjetas American Express, el código es un número de cuatro dígitos no grabado en relieve, sino impreso encima del PAN, en el anverso de todas las tarjetas de pago. El código se asocia de manera exclusiva a cada plástico individual y vincula el PAN al plástico. La siguiente lista especifica los términos según la marca de la tarjeta: ▪ **CID –** Card Identification Number (número de identificación de la tarjeta) (tarjetas de pago American Express y Discover) ▪ **CAV2 –** Card Authentication Value 2 (valor de autenticación de la tarjeta 2) (tarjetas de pago JCB) ▪ **PAN CVC2 –** Card Validation Code 2 (código de validación de la tarjeta 2) (tarjetas de pago MasterCard) ▪ **CVV2 –** Card Verification Value 2 (valor de verificación de la tarjeta 2) (tarjetas de pago Visa)
Titular de tarjeta	Cliente consumidor o no consumidor para el que se emite la tarjeta de pago, o cualquier individuo autorizado para utilizar una tarjeta de pago.

Término	Definición
Datos del titular de la tarjeta	Los datos del titular de la tarjeta contienen, como mínimo, el PAN completo. Es posible que los datos del titular de la tarjeta también incluyan el PAN completo más alguno de los siguientes datos: nombre del titular de la tarjeta, fecha de vencimiento y/o código de servicio Consulte *Datos confidenciales de autenticación* para obtener más información sobre elementos de datos que pueden transmitirse o procesarse, pero no procesarse, como parte de una transacción de pago.
CDE	Acrónimo de “cardholder data environment” (entorno de datos del titular de la tarjeta) Las personas, los procesos y la tecnología que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación.
Tecnologías celulares	Comunicaciones móviles mediante redes de teléfonos inalámbricos, entre otras, el sistema global de comunicaciones móviles (GSM), el acceso múltiple por división de código (CDMA) y el servicio de radio por paquetes generales (GPRS).
CERT	Acrónimo de “Computer Emergency Response Team” (Equipo de Respuesta ante Emergencias Informáticas) de la Universidad Carnegie Mellon. El programa del CERT desarrolla y promueve el uso de prácticas de administración de tecnología y sistemas apropiadas para resistir ataques a sistemas conectados en red, limitar daños y asegurar la continuidad de los servicios críticos.
Control de cambios	Procesos y procedimientos para revisar, probar y aprobar cambios a los sistemas y el software en función del impacto que puedan tener antes de su implementación.
CIS	Acrónimo de “Center for Internet Security” (centro de seguridad en Internet). Empresa sin fines de lucro cuya misión es ayudar a las organizaciones a reducir el riesgo de interrupciones en su negocio y en el comercio electrónico provocadas por controles de seguridad técnicos inadecuados.
Cifrado de bases de datos a nivel de columna	Técnica o tecnología (ya sea software o hardware) para cifrar el contenido de una columna específica de una base de datos y no todo el contenido de toda la base de datos. Consulte también *Cifrado de disco* o *Cifrado a nivel de archivo.*

Término	Definición
Controles de compensación	Es posible que los controles de compensación se consideren cuando una entidad no puede cumplir un requisito de manera explícita según lo establecido, debido a limitaciones técnicas legítimas o comerciales documentadas, pero ha mitigado de manera suficiente el riesgo asociado con el requisito a través de la implementación de controles. Los controles de compensación deben: (1) Cumplir con el propósito y el rigor del requisito original de las PCI DSS; (2) Proporcionar un nivel similar de defensa, como el requisito original de las PCI DSS; (3) Superar ampliamente otros requisitos de las PCI DSS (no simplemente en cumplimiento de otros requisitos de las PCI DSS); y (4) Ser cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS. Para obtener información acerca del uso de los controles de compensación, consulte los Anexos B y C de los Controles de compensación que se encuentran en los *Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad*.
Riesgo	También denominado “riesgo de datos” o “violación de datos”. Intrusión en un sistema de computadoras en la cual se sospecha una divulgación, un robo, una modificación o la destrucción no autorizada de datos del titular de la tarjeta.
Consola	Pantalla o teclado que permite obtener acceso al servidor, equipo mainframe u otro tipo de sistema y controlarlo dentro de un entorno de red.
Consumidor	Persona que compra bienes, servicios o ambos.
Sistemas críticos / tecnologías críticas	Un sistema o tecnología que la entidad considera de particular importancia. Por ejemplo, es posible que se requiera un sistema crítico para el desempeño de una operación comercial o para mantener una función de seguridad. Algunos ejemplos de sistemas críticos generalmente incluyen sistemas de seguridad, los dispositivos y sistemas públicos, las bases de datos y otros sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta. Las consideraciones para determinar cuáles sistemas o tecnologías específicos son críticos dependerán del entorno y la estrategia de evaluación de riesgos de una organización.
Falsificación de solicitudes entre distintos sitios (CSRF)	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que permiten que se ejecuten acciones no deseadas mediante una sesión que ha sido autenticada. Suele utilizarse junto con XSS o inyección SQL.
Lenguaje de comandos entre distintos sitios (XSS)	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada. Suele utilizarse junto con CSRF o inyección SQL.
Clave criptográfica	Valor que determina el resultado de un algoritmo de cifrado al transformar texto simple en texto cifrado. En general, la extensión de una clave determina la dificultad para descifrar el texto de un determinado mensaje. Consulte *Criptografía sólida.*

Término	Definición

Generación de claves criptográficas	La generación de claves es una de las funciones de la gestión de claves. Los siguientes documentos ofrecen una guía reconocida sobre cómo generar claves de manera apropiada:
	• NIST Special Publication 800-133: Recomendación para la Generación de claves criptográficas
	• ISO 11568-2 Servicios financieros — Gestión de claves (comercio minorista) — Parte 2: Cifrados simétricos, su gestión de claves y ciclo de vida
	  ○ 4.3 Generación de claves
	• ISO 11568-4 Servicios financieros — Gestión de claves (comercio minorista) — Parte 4: Criptosistemas asimétricos — Gestión de claves y ciclo de vida
	  ○ 6.2 Etapas del ciclo de vida de las claves — Generación
	• Pautas sobre el uso de algoritmos y gestión de claves EPC 342-08 del Consejo Europeo de Pagos
	  ○ 6.1.1 Generación de claves [para algoritmos simétricos]
	  ○ 6.2.1 Generación de claves [para algoritmos asimétricos]

Administración de claves criptográficas	Conjunto de procesos y mecanismos que respaldan el establecimiento y mantenimiento de las claves, así como el reemplazo de claves anteriores por nuevas claves, según sea necesario.
Criptografía	Disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.
Período de cifrado	Lapso de tiempo durante el cual se puede utilizar una clave criptográfica para su propósito definido basándose en, por ejemplo, un período de tiempo definido y/o la cantidad de texto cifrado producido, y según las mejores prácticas y directrices de la industria (por ejemplo, la *Publicación especial 800-57 del NIST*).
CVSS	Acrónimo de “Common Vulnerability Scoring System” (sistema de puntaje de vulnerabilidad común). Un estándar abierto y neutro de la industria para los proveedores cuya finalidad es transmitir la gravedad que presentan las vulnerabilidades en la seguridad de un sistema informático y ayudar a determinar tanto la urgencia como la prioridad de la respuesta. Para obtener más información, consulte la *Guía del programa ASV*.
Diagrama de flujo de datos	Diagrama que muestra de qué manera circulan los datos en una aplicación, un sistema o una red.
Base de datos	Formato estructurado que permite organizar y mantener información de fácil recuperación. Algunos ejemplos simples de base de datos son las tablas y las hojas de cálculo.
Administrador de bases de datos	También denominado “DBA”. Se refiere al responsable de administrar bases de datos.
Cuentas predeterminadas	Cuenta de inicio de sesión que se encuentra predefinida en un sistema, aplicación o dispositivo que permite obtener acceso por primera vez al momento en que el sistema comienza a funcionar. El sistema también puede generar cuentas predeterminadas adicionales como parte del proceso de instalación.

Término	Definición
Contraseña predeterminada	Contraseña de las cuentas de usuario, servicio o administración de sistemas predefinidas en un sistema, aplicación o dispositivo asociado con la cuenta predeterminada. Las contraseñas y cuentas predeterminadas son de dominio público y, en consecuencia, es fácil averiguarlas.
Destrucción magnética	También denominada "destrucción magnética de disco". Proceso o técnica que desmagnetiza un disco para destruir permanentemente toda la información almacenada en este.
Dependencia	En el contexto de las PA-DSS, una dependencia es un software o un componente de hardware específico (como una terminal de hardware, una base de datos, un sistema operativo, API, una biblioteca de códigos, etc.). que se necesita para que la aplicación de pago cumpla los requisitos de las PA-DSS.
Cifrado de disco	Técnica o tecnología (ya sea de software o hardware) que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). También se utiliza el *cifrado a nivel de archivo* o el *cifrado de bases de datos a nivel de columna* para cifrar el contenido de archivos o columnas específicas.
DMZ	Abreviatura de "demilitarized zone" (zona desmilitarizada). Subred física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización. La DMZ agrega una capa de seguridad de red adicional entre Internet y la red interna de una organización, de modo que las partes externas sólo tengan conexiones directas a los dispositivos de la DMZ y no a toda la red interna.
DNS	Acrónimo de "Domain Name System" (sistema de nombre de dominio) o "domain name server" (servidor de nombre de dominio). Sistema que almacena información relacionada con nombres de dominio en una base de datos distribuida en redes, como Internet.
DSS	Acrónimo de "Data Security Standard" (norma de seguridad de datos). Consulte *las PCI DSS* y *PA-DSS.*
Control dual	Proceso que consiste en utilizar dos o más entidades distintas (por lo general, personas) de manera coordinada para proteger funciones o información confidenciales. Ambas entidades son igualmente responsables de la protección física de los materiales que intervienen en transacciones vulnerables. Ninguna persona tiene permitido obtener acceso a o utilizar estos materiales (por ejemplo, la clave criptográfica). Para generar, transferir, cargar, almacenar y recuperar manualmente una clave, el proceso de control dual requiere que se divida el conocimiento de la clave entre las entidades. (Consulte también *Conocimiento parcial*).
Filtrado dinámico de paquetes	Consulte *Inspección completa.*
ECC	Acrónimo de "Elliptic Curve Cryptography" (criptografía de curva elíptica). Método de criptografía de clave pública basado en curvas elípticas sobre campos finitos. Consulte *Criptografía sólida.*
Filtrado de egreso	Método que permite filtrar el tráfico saliente de una red, de modo que sólo el tráfico explícitamente autorizado pueda salir de la red.

Término	Definición
Cifrado	Proceso para convertir información en un formato ilegible, a excepción de los titulares de una clave criptográfica específica. El cifrado se utiliza para proteger la información entre el proceso de cifrado y el proceso de descifrado (lo contrario del cifrado) de la divulgación no autorizada. Consulte *Criptografía sólida.*
Algoritmo de cifrado	También denominado "algoritmo criptográfico". Secuencia de instrucciones matemáticas usadas para transformar textos o datos no cifrados en textos o datos cifrados y viceversa. Consulte *Criptografía sólida.*
Entidad	Término utilizado para representar a la corporación, organización o negocio bajo una revisión de las PCI DSS.
Supervisión de la integridad de archivos	Técnica o tecnología utilizada para supervisar archivos o registros a fin de detectar si se modificaron. Si se modifican archivos o registros críticos, se debería enviar mensajes de alerta al personal de seguridad apropiado.
Cifrado a nivel de archivo	Técnica o tecnología (ya sea software o hardware) para cifrar todo el contenido de archivos específicos. Consulte también *Cifrado de disco* o *Cifrado de bases de datos a nivel de columna.*
FIPS	Acrónimo de "Federal Information Processing Standards" (normas de procesamiento de información federal de los EE. UU.). Normas aceptadas públicamente por el gobierno federal de los EE. UU., a disposición también de agencias no gubernamentales y contratistas.
Firewall	Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tráfico de computadoras entre redes con diferentes niveles de seguridad basándose en un conjunto de reglas y otros criterios.
Herramientas forenses	También se denomina "ciencia forense informática". Cuando se trata de la seguridad de la información, se refiere a la aplicación de herramientas de investigación y técnicas de análisis para recolectar evidencia a partir de recursos informáticos a fin de determinar la causa del riesgo de los datos.
FTP	Acrónimo de "File Transfer Protocol" (protocolo de transferencia de archivos). Protocolo de red que se utiliza para transferir datos de una computadora a otra mediante un red pública, como Internet. En general, se considera que FTP es un protocolo inseguro, porque permite enviar contraseñas y contenido de archivos sin protección y en texto simple. El protocolo FTP puede implementarse con seguridad mediante SSH u otra tecnología. Consulte *S-FTP*.
GPRS	Acrónimo de "General Packet Radio Service" (servicio de radio paquete general) Servicio de datos portátil disponible para los usuarios de teléfonos móviles GSM. Reconocido por el uso eficaz de un ancho de banda limitado. Ideales para enviar y recibir pequeños paquetes de datos, como correos electrónicos y para navegar en Internet.
GSM	Acrónimo de "Global System for Mobile Communications" (sistema global de comunicaciones móviles). Norma ampliamente difundida para teléfonos móviles y redes. La ubicuidad de la norma GSM convierte el acceso de llamada itinerante o "roaming" a nivel internacional en algo muy común entre los operadores de telefonía inalámbrica, lo que permite a los suscriptores utilizar sus teléfonos en distintos lugares del mundo.

Término	Definición
Hashing	Proceso que vuelve ilegibles los datos de titulares de tarjetas convirtiendo los datos en un resumen de mensaje de longitud fija. . El hashing es una función (matemática) en la cual un algoritmo conocido toma un mensaje de longitud arbitraria como entrada y produce un resultado de longitud fija (generalmente denominado “código hash” o “resumen de mensaje”). Una función hash debe tener las siguientes propiedades: (1) Que no se pueda determinar informáticamente la entrada original si sólo se tiene el código hash, (2) Que no se puedan hallar informáticamente dos entradas que generen el mismo código hash. En el contexto de las PCI DSS, la función hash se debe aplicar a todo el PAN para que se considere que el código hash es ilegible. Se recomienda que los datos de titulares de tarjetas en valores hash incluyan un valor de entrada (por ejemplo, un valor de "sal") en la función de hashing para reducir o disminuir la efectividad de los ataques de las tablas rainbow computadas previamente (consulte *Variable de entrada*). Si desea más orientación, consulte otras normas de la industria, tales como las versiones actuales de NIST Special Publications 800-107 y 800-106, Federal Information Processing Standard (FIPS) 180-4 Secure Hash Standard (SHS) y FIPS 202 SHA-3 Standard: Funciones de hash basado en permutación y de salida extensible.
Host	Computadora principal donde reside el software informático.
Proveedor de hosting	Ofrece diferentes servicios a comerciantes y otros proveedores de servicios. Los servicios van de simples a complejos: desde un espacio compartido en un servidor hasta una completa gama de opciones para el “carrito de compras”; desde aplicaciones de pago hasta conexiones con pasarelas y procesadores de pago; y para proveer servicio de hosting dedicado sólo a un cliente por servidor. Es posible que el proveedor de hosting sea un proveedor de hosting compartido, encargado de prestar servicio a diferentes entidades en un solo servidor.
HSM	Acrónimo de “hardware security module” (módulo de seguridad de hardware) o “host security module” (módulo de seguridad de host). Un dispositivo de hardware protegido en forma lógica y física que proporciona un conjunto seguro de servicios cartográficos, empleados en funciones de administración de claves criptográficas o el descifrado de los datos de cuentas.
HTTP	Acrónimo de “hypertext transfer protocol” (protocolo de transferencia de hipertexto). Protocolo abierto de Internet que permite transferir o transmitir información en la World Wide Web.
HTTPS	Acrónimo de “hypertext transfer protocol over secure socket layer” (protocolo de transferencia de hipertexto a través de una capa de conexión segura). HTTP seguro que proporciona autenticación y comunicación cifrada en la World Wide Web diseñado para comunicaciones que dependen de la seguridad, tales como los inicios de sesión basados en la web.

Término	Definición
Hipervisor	Software o firmware responsable de prestar servicios de hosting a máquinas virtuales y administrarlas. En cuanto a las PCI DSS, el componente del sistema hipervisor también incluye el VMM, virtual machine monitor (supervisor de máquinas virtuales).
ID	Identificador correspondiente a un usuario o una aplicación particular.
IDS	Acrónimo de "intrusion detection system" (sistema de detección de intrusiones). Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en una base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad detectado. Consulte *IPS*
IETF	Acrónimo de "Internet Engineering Task Force" (grupo de trabajo de ingeniería en Internet). Comunidad internacional abierta y extensa de diseñadores de redes, operadores, proveedores e investigadores que trabajan en el desarrollo de la arquitectura de Internet y se ocupan de su correcto funcionamiento. El IETF no exige la acreditación de membresías y está abierto a cualquier persona interesada.
IMAP	Acrónimo de "Internet Message Access Protocol" (protocolo de acceso de mensajes de Internet). Protocolo de Internet de capa de aplicación que permite a un cliente de correo electrónico acceder a los mensajes almacenados en un servidor de correo remoto.
Token de índice	Token criptográfico que, basado en un índice dado para un valor imprevisible, reemplaza el PAN.
Seguridad de la información	Protección de la información que garantiza la confidencialidad, integridad y disponibilidad.
Sistema de información	Conjunto específico de recursos de datos estructurados organizados para recolectar, procesar, mantener, usar, compartir, diseminar o disponer de la información.
Filtrado de ingreso	Método que permite filtrar el tráfico entrante de una red, de modo que sólo el tráfico explícitamente autorizado pueda ingresar a la red.
Errores de inyección	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web. En esta clase de vulnerabilidades se incluye la inyección SQL, la inyección LDAP y la inyección XPath.
Variable de entrada	Cadena aleatoria de datos que se concatena con datos de origen antes de que una función unidireccional hash la afecte. Las variables de entrada pueden ayudar a reducir la efectividad de los ataques de tablas rainbow. Consulte también *Hashing* y *Tablas rainbow.*

Término	Definición
Protocolo/Servicio/Puerto no seguros	Un protocolo, servicio o puerto que produce preocupación en cuanto a la seguridad debido a la falta de controles de confidencialidad y/o integridad. Estas preocupaciones relacionadas con la seguridad afectan a los servicios, protocolos o puertos que transmiten datos o credenciales de autenticación (como contraseñas o frases de seguridad) de texto simple en Internet, o son fáciles de explotar si se configuran incorrectamente o de forma predeterminada. Entre los servicios, protocolos o puertos inseguros, se incluyen, a modo de ejemplo, FTP, Telnet, POP3, IMAP y SNMP versión 1 y versión 2.
IP	Acrónimo de "internet protocol" (protocolo de Internet). Protocolo de capas de red que contiene información sobre direcciones y algunos datos de control, y permite el ruteo de paquetes y se envían desde el alojamiento de origen al alojamiento de destino. IP es el protocolo primario de capas de red en la suite de protocolos de Internet. Consulte *TPC*.
Dirección IP	También denominada "dirección de protocolo de Internet". Código numérico que identifica exclusivamente una computadora en Internet.
Falsificación de dirección IP	Técnica de ataque utilizada para obtener acceso no autorizado a redes o computadoras. La persona malintencionada envía mensajes engañosos a una computadora. Los mensajes tienen una dirección IP que indica que el mensaje proviene de un host de confianza.
IPS	Acrónimo de "intrusion prevention system" (sistema de prevención de intrusiones). El IPS va un paso más allá que el IDS y bloquea el intento de intrusión.
IPSEC	Abreviatura de "Internet Protocol Security" (protocolo de seguridad de Internet). Norma para asegurar las comunicaciones IP mediante el cifrado y/o la autenticación de todos los paquetes IP.
ISO	En el contexto de normas industriales y mejores prácticas, ISO, mejor conocida como la "Organización Internacional para la Estandarización" es una organización no gubernamental que consta de una red de institutos nacionales de normalización.
Emisor	Entidad que emite tarjetas de pago o realiza, facilita o respalda servicios de emisión incluidos, a modo de ejemplo, bancos y procesadores emisores. También denominado "banco emisor" o "instituciones financieras emisoras".
Servicios de emisión	Entre los ejemplos de servicios de emisión se pueden incluir, a modo de ejemplo, la autorización y la personalización de tarjetas.
LAN	Acrónimo de "local area network" (red de área local). Grupo de computadoras y/u otros dispositivos que comparten una línea de comunicaciones común, generalmente, en un edificio o grupo de edificios.
LDAP	Acrónimo de "Lightweight Directory Access Protocol" (protocolo ligero de acceso directo). Repositorio de datos para la autenticación y autorización destinado a las consultas y modificaciones relativas a permisos de usuario y al otorgamiento de derechos de acceso a recursos protegidos.

Término	Definición
Menor cantidad de privilegios	Contar con el acceso o los privilegios mínimos necesarios de cada función para que puedan desempeñar sus funciones y responsabilidades.
Registro	Consulte *Registro de auditoría.*
LPAR	Abreviatura de “logical partition” (partición lógica). Sistema de subdivisión o partición de todos los recursos de una computadora (procesadores, memoria y almacenamiento) en unidades más pequeñas, capaces de ejecutarse con una copia propia distinta del sistema operativo y de las aplicaciones. En general, la partición lógica se utiliza para facilitar el uso de varios sistemas operativos y aplicaciones en un mismo dispositivo. Es posible, aunque no obligatorio, configurar las particiones para que se comuniquen entre sí o compartan algunos recursos del servidor, como las interfaces de red.
MAC	En criptografía, acrónimo de “message authentication code” (código de autenticación de mensajes). Información breve que se utiliza para autenticar un mensaje. Consulte *Criptografía sólida.*
Dirección MAC	Abreviatura de “media access control address” (dirección de control de acceso a medios). Valor único de identificación que el fabricante asigna a los adaptadores de red y a las tarjetas de interfaz de red.
Datos de la banda magnética	Consulte *Datos de la pista.*
Mainframe	Computadoras diseñadas para trabajar con grandes volúmenes de entrada y salida de datos y para enfatizar el rendimiento informático. Los sistemas mainframe pueden ejecutar varios sistemas operativos, por lo que parece que estuvieran operando como múltiples computadoras. Muchos sistemas heredados presentan un diseño de mainframe.
Software malicioso o malware	Software o firmware desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema. Algunos ejemplos son los virus, gusanos, troyanos (o caballos de Troya), spyware, adware y rootkits.
Ocultamiento	En el contexto de las PCI DSS, se refiere al método para ocultar un segmento de los datos cuando se muestran o imprimen. El ocultamiento se utiliza cuando no existe un requisito por parte del negocio de ver el PAN completo. El ocultamiento se relaciona con la protección del PAN cuando se muestra o imprime. Consulte *Truncamiento* para obtener información sobre la protección del PAN cuando se almacena en archivos, bases de datos, etc.
Ataques para extraer la memoria	Actividad de malware que se dedica a examinar y extraer los datos almacenados en la memoria mientras se procesan, o que no se han sobrescrito apropiadamente.

Término	Definición
Comerciante	En lo que concierne a las PCI DSS, comerciante se define como toda entidad que acepta tarjetas de pago con el logotipo de cualquiera de los cinco miembros del PCI SSC (American Express, Discover, JCB, MasterCard o Visa) como forma de pago por bienes y servicios. Tenga en cuenta que un comerciante que acepta tarjetas de pago por bienes y servicios puede ser también un proveedor de servicios, si los servicios comerciados tienen como resultado almacenamiento, procesamiento o transmisión de datos de titulares de tarjetas a nombre de otros comerciantes o proveedores de servicios. Por ejemplo, puede que un ISP sea un comerciante que acepte tarjetas pago por facturaciones mensuales, pero que, si los clientes para los que actúa como host son comerciantes, sea al mismo tiempo proveedor de servicios.
MO/TO	Acrónimo de “Mail-Order/Telephone-Order” (pedidos por correo/teléfono)
Supervisión	Uso de sistemas o procesos que constantemente vigilan los recursos de computadoras o redes a efectos de alertar al personal en caso de interrupciones, alarmas u otros eventos predefinidos.
MPLS	Acrónimo de “multi protocol label switching” (conmutación multiprotocolo mediante etiquetas). Mecanismo de red o telecomunicaciones diseñado para conectar un grupo de redes basadas en la conmutación de paquetes.
Autenticación de múltiples factores	Método de autenticación de un usuario mediante la comprobación de por lo menos dos 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).
NAC	Acrónimo de “network access control” (control de acceso de red) o “network admission control” (control de admisión de red). Método de implementación de seguridad en la capa de red mediante la restricción de la disponibilidad de los recursos de la red para los dispositivos de extremo, según una política de seguridad definida.
NAT	Acrónimo de “network address translation” (traducción de direcciones de red). Llamada también simulación de red o simulación IP. Cambio de dirección de IP usada dentro de una red por una dirección de IP diferente conocida dentro de otra red, lo que permite que una organización tenga direcciones internas que solo son visibles dentro de la red y direcciones externas que solo son visibles fuera de la red.
Red	Dos o más computadoras interconectadas a través de un medio físico o inalámbrico.
Administrador de red	Personal responsable de administrar la red dentro de una entidad. Entre las responsabilidades generalmente se incluyen, a modo de ejemplo, la seguridad, las instalaciones, las actualizaciones, el mantenimiento y la monitorización de la actividad de la red.
Componentes de red	Los componentes de la red incluyen, a modo de ejemplo, firewalls, conmutadores, routers, puntos de acceso inalámbrico, aplicaciones de red y otras aplicaciones de seguridad.

Término	Definición
Diagrama de una red	Diagrama que muestra los componentes del sistema y las conexiones existentes dentro de un entorno en red.
Análisis de seguridad de la red	Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas.
Segmentación de red	También llamada “segmentación” o “aislamiento”. La segmentación de red separa componentes del sistema que almacenan, procesan o transmiten datos del titular de la tarjeta de sistemas que no lo hacen. Una segmentación de red adecuada puede reducir el alcance del entorno de los datos del titular de la tarjeta y, por lo tanto, reducir el alcance de la evaluación de las PCI DSS. Consulte la sección Segmentación de red en *Requisitos de las DSS PCI y procedimientos de evaluación de seguridad* para obtener información acerca del uso de segmentación de red. La segmentación de red no es un requisito de las PCI DSS.
Detector de red	También llamado “detector de paquete” o “detector”. Técnica que en forma pasiva monitorea o recopila comunicaciones de red, decodifica protocolos y examina el contenido para obtener información de interés.
NIST	Acrónimo de “National Institute of Standards and Technology” (Instituto Nacional de Normas y Tecnología). Agencia federal no regulatoria dependiente de la Administración Tecnológica del Departamento de Comercio de los Estados Unidos.
NMAP	Software para el análisis de riesgos de seguridad encargado de delinear redes e identificar puertos abiertos en los recursos de red.
Acceso que no sea de consola	Se refiere al acceso lógico a un componente del sistema que tiene lugar a través de una interfaz de red en lugar de serlo mediante una conexión física y directa con el componente del sistema. El acceso que no es de consola incluye el acceso desde el interior de las redes internas/locales así como el acceso desde redes externas, o remotas.
Usuarios no consumidores	Todas las personas, con excepción de los titulares de tarjetas, que tengan acceso a los componentes de sistema, entre los cuales se incluyen empleados, administradores y terceros.
NTP	Acrónimo de “network time protocol” (Protocolo de tiempo de red). Protocolo usado para sincronizar los relojes de sistemas informáticos, dispositivos de red y otros componentes del sistema.
NVD	Acrónimo de “National Vulnerability Database” (base de datos nacional de vulnerabilidades). Depósito del gobierno de los EE. UU. de los datos de administración de vulnerabilidades basados en estándares. NVD incluye bases de datos de listas de verificación de seguridad, fallas en los programas de software relacionadas con la seguridad, las configuraciones incorrectas, los nombres de productos y las métricas de las incidencias.

Término	Definición
OCTAVE®	Acrónimo de “Operationally Critical Threat, Asset, and Vulnerability Evaluation” (Evaluación de vulnerabilidades, activos y amenazas críticos operativamente). Un conjunto de herramientas, técnicas y métodos para la evaluación y la planificación estratégicas de seguridad de la información basadas en riesgos.
Productos estándar	Descripción de productos listos para usar comercializados como bienes no personalizadas o específicamente diseñadas para un cliente o usuario.
Sistema operativo / OS	Software de un sistema de computadoras a cargo de compartir recursos informáticos y administrar y coordinar todas las actividades informáticas. Algunos ejemplos de sistemas operativos incluyen Microsoft Windows, Mac OS, Linux y Unix.
Independencia organizativa	Estructura organizativa que garantiza la ausencia de conflicto de intereses entre la persona o el departamento que lleva a cabo una actividad, y la personal o el departamento encargado de evaluarla. Por ejemplo, las personas que realicen las evaluaciones deben estar separados, desde el punto de vista organizativo, de la administración del entorno que se está evaluando.
OWASP	Acrónimo de “Open Web Application Security Project” (Guía para proyectos de seguridad de aplicaciones web abiertas). Es una organización sin fines de lucro especializada en mejorar la seguridad del software de aplicación. OWASP mantiene una lista con las vulnerabilidades más críticas de las aplicaciones web. (Consulte http://www.owasp.org).
PA-DSS	Acrónimo de “Payment Application Data Security Standard” (Norma de Seguridad de Datos para las Aplicaciones de Pago).
PA-QSA	Acrónimo de “Payment Application Qualified Security Assessor” (Asesor de Seguridad Certificado para las Aplicaciones de Pago). Los PA-QSA están calificados por las PCI SSC para realizar evaluaciones de aplicaciones de pago de acuerdo con las PA-DSS. Consulte la *Guía del programa de PA-DSS* y los *Requisitos de Calificación del PA-QSA* para obtener detalles respecto de los requisitos para las empresas y empleados de PA-QSA.
Ensambladores	En la criptografía, el ensamblador de un solo uso es un algoritmo de cifrado con texto que se combina con una clave aleatoria o "ensamblador". Presenta una extensión igual a la del texto simple y puede utilizarse solo una vez. Asimismo, si la clave es en verdad aleatoria, secreta y de un solo uso, no será posible descifrar el ensamblador
PAN	Acrónimo de “primary account number” (número de cuenta principal), también denominado “número de cuenta”. Número exclusivo de una tarjeta de pago (en general, de tarjetas de crédito o débito) que identifica al emisor y la cuenta específica del titular de la tarjeta.
Consultas basadas en parámetros	Un medio de estructuración de consultas SQL para limitar un escape y, por lo tanto, impedir ataques de inyección.
Contraseña / frase de seguridad	Una serie de caracteres que autentican la identidad del usuario.

Término	Definición
PAT	Acrónimo de “port address translation” (traducción de dirección de puertos) o “traducción de dirección de puertos de red”. Tipo de *NAT* que además traduce números de puertos.
Parche	Actualización de un software existente para agregarle funcionalidad o corregir un defecto.
Aplicación de pago	En el contexto de las PA-DSS, una aplicación de software que almacena, procesa o transmite datos de titulares de tarjetas como parte de la autorización o de la liquidación, cuando dicha aplicación de pago se vende, distribuye u otorga bajo licencia a terceros. Para obtener detalles, consulte la *Guía del programa de las PA-DSS*.
Tarjetas de pago	En lo que concierne a las PCI DSS, toda tarjeta de pago o dispositivo que lleve el logotipo de los miembros fundadores de las PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide o Visa Inc.
Procesador de pago	Algunas veces denominada “puerta de enlace de pago” o “proveedor de servicio de pago (PSP)”. Entidad contratada por un comerciante u otra entidad para manejar transacciones con tarjetas de pago en su nombre. Si bien los procesadores de pago generalmente adquieren servicios de pago, los procesadores de pago no son considerados adquirientes, a menos que así lo defina una marca de tarjeta de pago. Ver también *Adquiriente.*
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).
PDA	Acrónimo de “personal data assistant” (asistente de datos personal) o “personal digital assistant” (asistente digital personal). Dispositivo portátiles manuales que funcionan como teléfonos móviles, redactores de correos electrónicos y exploradores web.
PED	Acrónimo de "PIN entry device" (dispositivo de entrada de PIN).
Prueba de penetración	Las pruebas de penetración tienen como finalidad intentar identificar maneras de aprovechar las vulnerabilidades para evitar o rechazar las características de seguridad de los componentes del sistema. Las pruebas de penetración incluyen pruebas de aplicaciones y de redes, y controles y procesos de redes y aplicaciones. Se realizan tanto desde el exterior del entorno (pruebas externas) como en el sentido contrario.
Software de firewall personal	Un firewall de software instalado en una única computadora.
Información de identificación personal	Información que se puede utilizar para identificar y rastrear a una persona entre otras, pero sin limitarse a, nombre, dirección, número del seguro social, datos biométricos, número de teléfono, etc.
Personal	Empleados de tiempo completo y parcial, empleados temporales, y contratistas y consultores que “residan” en las instalaciones de la entidad o que de alguna otra forma tengan acceso al entorno de datos de titulares de tarjetas.

Término	Definición
PIN	Acrónimo de “personal identification number” (número de identificación personal). Contraseña numérica secreta que conocen solo el usuario y un sistema para autenticar al usuario en el sistema. El usuario tan solo obtiene acceso si su PIN coincide con el PIN del sistema. Los PIN más comunes se utilizan en las transacciones de adelanto de efectivo y las ATM. Otro tipo de PIN es el que utilizan las tarjetas con chip de tipo EMV, en las que el PIN reemplaza la firma del titular de la tarjeta.
Bloqueo de PIN	Un bloqueo de datos utilizado para encapsular un PIN durante el procesamiento. El formato del bloqueo de PIN define el contenido de dicho bloqueo y cómo se procesa para recuperar el PIN. El bloqueo de PIN consta del PIN, la longitud de PIN y puede contener un subconjunto del PAN.
POI	Acrónimo de “Point of Interaction” (Punto de interacción), el punto inicial en que se leen los datos de una tarjeta. Un POI, un producto de transacción-aceptación electrónica, consta de hardware y software y se hospeda en el equipo de aceptación para permitir al titular realizar una transacción con la tarjeta. El POI puede estar supervisado o no supervisado. Las transacciones de POI suelen ser transacciones de pago basadas en tarjeta con circuito integrado (chip) y/o banda magnética.
Política	Normas vigentes para toda la organización que reglamentan el uso aceptable de los recursos informáticos, las prácticas de seguridad y el desarrollo guiado de procedimientos operacionales.
POP3	Acrónimo de “Post Office Protocol v3” (Protocolo de oficina postal v3). Protocolo de capa de aplicación que permite a un cliente de correo electrónico recuperar los mensajes almacenados en un servidor remoto a través de una conexión de TCP/IP.
Puerto	Puntos de conexión lógicos (virtuales) asociados con un protocolo de comunicación particular para facilitar las comunicaciones entre redes.
POS	Acrónimo de “point of sale” (punto de venta). Hardware y/o software que se utiliza para procesar transacciones con tarjetas de pago en la ubicación del comerciante.
Red privada	Red establecida por una organización que utiliza un espacio de dirección IP privado. Generalmente, a las redes privadas se las denomina redes de área local. El acceso a redes privadas desde redes públicas debe estar protegido adecuadamente mediante firewalls y routers. Ver también *Red pública*.
Usuario con privilegios	Cualquier cuenta de usuario que posee privilegios de acceso que superan los privilegios básicos. Por lo general, estas cuentas tienen privilegios mayores o aumentados con más derechos que una cuenta de usuario estándar. No obstante, la gama de privilegios otorgados en las diferentes cuentas con privilegios pueden variar ampliamente, según sea la organización, la función o el puesto de trabajo y la tecnología que se usa.
Procedimiento	Narración descriptiva de una política. El procedimiento equivale a los pasos de una política y describe cómo debe implementarse una determinada política.

Término	Definición
Protocolo	Método acordado de comunicación utilizado en las redes. Son las especificaciones que describen las reglas y los procedimientos que deben seguir los diferentes productos informáticos para realizar actividades en una red.
Servidor proxy	Servidor que funciona como intermediario entre una red interna e Internet. Por ejemplo, una función de un servidor proxy es finalizar o negociar las conexiones entre las conexiones internas y externas, de manera tal que cada una solamente se comunica con el servidor proxy.
PTS	Acrónimo de "PIN Transaction Security" (Seguridad de la transacción con PIN), PTS es un conjunto de requisitos de evaluación modular administrados por el PCI Security Standards Council, para terminales POI con aceptación de PIN. Por favor, consulte www.pcisecuritystandards.org.
Red pública	Red específicamente implementada y operada por un proveedor de telecomunicaciones de tercero con el propósito de ofrecer al público servicios de transmisión de datos. Los datos que se transfieren por medio de redes públicas pueden ser interceptados, modificados y/o redirigidos mientras están en tránsito. Algunos de los ejemplos de redes públicas son Internet y las tecnologías móviles e inalámbricas. Ver también *Red privada*.
PVV	Acrónimo de "PIN verification value" (valor de verificación de PIN). Valor discrecional codificado en la banda magnética de una tarjeta de pago.
QIR	Acrónimo de "Qualified Integrator or Reseller" (integrador o revendedor certificado). Para obtener más información, consulte la *Guía del programa QIR* en el sitio web de PCI SSC.
QSA	Acrónimo de "Qualified Security Assessor" (Asesor de Seguridad Certificado). Los QSA están calificados por las PCI SSC para realizar evaluaciones en el lugar. Consulte los *Requisitos de calificación* para obtener detalles respecto de los requisitos para las empresas y los empleados de QSA.
RADIUS	Abreviatura de "remote authentication and dial-in user service" (autenticación remota y servicio dial-in del usuario). Sistema de autenticación y cuentas. Comprueba que la información transferida al servidor RADIUS, como el nombre de usuario y la contraseña, sea correcta, para autorizar luego el acceso al sistema. Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de múltiples factores.
Ataque de tablas rainbow	Método de ataque de datos que utiliza una tabla computarizada previa de cadenas de hash (resumen de mensaje de longitud fija) para identificar la fuente de datos original, usualmente mediante el craqueo de la contraseña o los hashes de datos del titular de la tarjeta.
Redigitación de clave	Proceso que consiste en el cambio de las claves criptográficas. La redigitación periódica de clave limita la cantidad de datos que pueden cifrarse con una misma clave.
Acceso remoto	Acceso a redes de computadoras desde una ubicación externa a esa red. Las conexiones de acceso remoto pueden originarse tanto desde la red propia de la empresa como de una ubicación remota que se encuentra por fuera de la red de la empresa. Las redes *VPN* constituyen un ejemplo de tecnologías de acceso remoto.

Término	Definición
Entorno de laboratorio remoto	Laboratorio que no es mantenido por el PA-QSA.
Medios electrónicos extraíbles	Medios capaces de almacenar datos digitalizados fáciles de extraer y transportar de un sistema informático a otro. Algunos ejemplos de medios electrónicos extraíbles incluyen CD-ROM, DVD-ROM, unidades flash USB y unidades de disco duro externas/portátiles.
Revendedor / integrador	Una entidad que vende y/o integra aplicaciones de pago, pero no las desarrolla.
RFC 1918	La norma identificada por el grupo de trabajo de ingeniería en Internet (IETF) que define el uso y la serie de direcciones apropiada para redes privadas (no ruteables en Internet).
Análisis de riesgos / Evaluación de riesgos	Proceso que identifica los recursos valiosos de un sistema y sus amenazas; cuantifica la exposición a pérdida (es decir, el potencial de pérdida) según frecuencias estimadas y costos derivados por siniestros; y, opcionalmente, recomienda el modo de asignar recursos como medidas preventivas que minimicen el índice total de exposición.
Clasificación de riesgos	Un criterio definido de medición en función de la evaluación de riesgos y el análisis de riesgos realizados a una entidad dada.
ROC	Acrónimo de “Report on Compliance” (informe de cumplimiento). Informe que describe detalles relacionados al estado de cumplimiento de las normas PCI DSS por parte de una entidad.
Rootkit	Tipo de software malicioso que, al instalarse sin autorización, es capaz de pasar desapercibido y tomar el control administrativo de un sistema informático.
Router	Hardware o software que conecta el tráfico entre dos o más redes. Clasifica e interpreta la información mediante la comprobación de direcciones y transmisión de bits de datos a los destinos correctos. Algunas veces se denomina puerta de enlace al software de un router.
ROV	Acrónimo de “Report on Validation” (informe de validación). Informe que describe detalles de una evaluación de las PA-DSS relacionados con el programa de las PA-DSS.
RSA	Algoritmo para criptografía asimétrica descripto en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT (Massachusetts Institute of Technology). Las letras RSA corresponden a las iniciales de sus nombres.
S-FTP	Acrónimo de “Secure-FTP” (FTP seguro). S-FTP posee la capacidad de cifrar la información de autenticación y los archivos de datos en tránsito. Consulte *FTP.*
Muestreo	El proceso de seleccionar una sección transversal de un grupo que es representativa de todo el grupo. El muestreo puede ser utilizado por asesores para reducir esfuerzos de pruebas generales, cuando se ha validado que en una entidad se han implementado procesos y controles de seguridad y operativos de las PCI DSS regulares y centralizados. El muestreo no es un requisito de las PCI DSS.

Término	Definición
SANS	Acrónimo de “SysAdmin, Audit, Networking and Security” (Administración de sistemas, auditorias, redes y seguridad), un instituto especialista en capacitación en seguridad informática y certificación profesional. (Consulte www.sans.org.)
SAQ	Acrónimo de “Self-Assessment Questionnaire” (Cuestionario de autoevaluación). Herramienta de generación de informes que describe los resultados de la autoevaluación a partir de la evaluación de las PCI DSS por parte de una entidad.
Esquema	Descripción formal respecto de la construcción de una base de datos, en la que se incluye la organización de los elementos que componen los datos.
Alcance	Proceso de identificación de todos los componentes del sistema, las personas y los procesos que se incluirán en una evaluación de las PCI DSS. El primer paso de una evaluación de las PCI DSS es determinar con exactitud el alcance de la revisión.
SDLC	Acrónimo de “system development life cycle” (ciclo de vida de desarrollo del sistema). Etapas del desarrollo de un software o sistema informático que incluye el planificación, análisis, diseño, pruebas e implementación.
Codificación segura	El proceso de creación e implementación de aplicaciones resistentes a alteración y/o exposición a riesgos.
Dispositivo seguro criptográfico	Un conjunto de hardware, software y firmware que implementa procesos criptográficos (incluidos algoritmos criptográficos y generación de claves) y que está contenido dentro de un límite criptográfico definido. Entre los ejemplos de dispositivos criptográficos seguros se incluyen los módulos de seguridad de hardware o de host (HSM) y dispositivos de punto de interacción (POI) que se han validad mediante los PCI PTS.
Limpieza segura	También llamado "borrado seguro", es un método de sobrescritura de los datos que se encuentran en un disco duro o en otro medio digital, lo que impide la recuperación de los datos.
Evento de seguridad	Una ocurrencia que una organización considera que posee implicaciones potenciales a la seguridad de un sistema o su entorno. En el contexto de las PCI DSS, los eventos de seguridad identifican aquella actividad que es sospechosa o anormal.
Jefe de seguridad	Principal responsable de los asuntos relacionados con la seguridad de una entidad.
Política de seguridad	Conjunto de leyes, reglamentos y prácticas que regulan el modo en una organización administra, protege y distribuye información confidencial.
Protocolos de seguridad	Protocolos de comunicaciones de red diseñados para asegurar la transmisión de datos. Algunos ejemplos de protocolos de seguridad son, sin limitarse a, TLS, IPSEC, SSH, HTTPS, etc.
Área confidencial	Todo centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenan, procesan o transmiten datos de titulares de tarjetas. No se incluyen las áreas en las que se encuentran presentes terminales de punto de venta, tales como el área de cajas en un comercio.

Término	Definición
Datos confidenciales de autenticación	Información de seguridad (entre otra, códigos o valores de validación de tarjetas, datos completos de la pista [de la banda magnética o su equivalente en un chip], PIN y bloqueos de PIN) utilizada en la autenticación de titulares de tarjetas o en la autorización de transacciones realizadas con tarjeta de pago.
Separación de funciones	Práctica que consiste en dividir los pasos de una función entre varias personas para evitar que un solo individuo pueda arruinar todo el proceso.
Servidor	Computadora que presta servicios a otras computadoras, como el procesamiento de comunicaciones, almacenamiento de archivos y acceso a impresoras. Los servidores incluyen entre otros: web, base de datos, aplicaciones, autenticación, DNS, correo, proxy y protocolos NTP.
Código de servicio	Código de valor de tres o cuatro dígitos en la banda magnética junto a la fecha de vencimiento de la tarjeta de pago presente en la pista de datos. Se utiliza, entre otras cosas, para definir atributos del servicio, diferenciar entre intercambios nacionales e internacionales e identificar restricciones de uso.
Proveedor de servicios	Entidad comercial diferente de una marca de pago que está directamente implicada en el procesamiento, el almacenamiento o la transmisión de los datos del titular de la tarjeta en nombre de otra entidad. Se incluyen también empresas que proveen servicios que controlan o pueden tener injerencia en la seguridad de los datos del titular de la tarjeta. Algunos ejemplos incluyen proveedores de servicios administrados que proveen firewalls gestionados, IDS y otros servicios; proveedores de hosting y otras entidades. Si una entidad proporciona un servicio que *solamente* implica la entrega de acceso a una red pública (por ejemplo, una empresa de telecomunicaciones que brinda solamente el vínculo de comunicación), la entidad no se consideraría un proveedor de servicios por ese servicio (si bien se la puede considerar como tal por otros servicios).
Token de sesión	En el contexto de gestión de sesiones web, un token de sesión (también conocido como “identificador de sesión” o “ID de sesión”), es un identificador único (como una “cookie”) que se utiliza para rastrear una sesión particular entre un explorador web y un servidor web.
SHA-1/SHA-2	Acrónimo de “Secure Hash Algorithm” (Algoritmo de hashing seguro). Una familia o un conjunto de funciones criptográficas de ordenamiento relacionadas, que incluye SHA-1 y SHA-2. Consulte *Criptografía sólida.*
Tarjeta inteligente	También denominada “tarjeta con chip” o “tarjeta IC (tarjeta de circuito integrado)”. Un tipo de tarjeta de pago que tiene circuitos integrados insertos en su interior. Estos circuitos, también llamados el “chip”, contienen datos de la tarjeta de pago entre los cuales se cuentan los datos equivalentes a los datos de banda magnética.
SNMP	Acrónimo de “Simple Network Management Protocol” (Protocolo simple de administración de red). Admite la monitorización de dispositivos conectados a una red dada cualquier condición que justifique atención administrativa.
Conocimiento parcial	Método mediante el cual dos o más entidades separadas poseen componentes de una clave, pero que, de forma individual, no pueden descifrar la clave criptográfica resultante.

Término	Definición
Spyware	Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.
SQL	Acrónimo de “Structured Query Language” (Lenguaje de consulta estructurado). Lenguaje informático utilizado para crear, modificar y recuperar datos de sistemas de administración de bases de datos relacionales.
Inyección SQL	Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.
SSH	Abreviatura de “secure shell”. Conjunto de protocolos que proporcionan cifrado de servicios de red, como inicio de sesión remoto o transferencia remota de archivos.
SSL	Acrónimo de “secure sockets layer” (capa de conexión segura). Norma de la industria que cifra el canal entre un explorador web y un servidor web. Ahora reemplazada por TLS. Consulte *TLS.*
Inspección completa	También denominada “dynamic packet filtering” (filtrado dinámico de paquetes). Firewall que, al realizar un seguimiento del estado de las conexiones de la red, proporciona una seguridad mejorada. Al estar programado para distinguir los paquetes legítimos de las diversas conexiones, el firewall permitirá solamente aquellos paquetes que coinciden con una conexión establecida, y rechazará a todos los demás.
Criptografía sólida	Criptografía basada en algoritmos probados y aceptados por la industria, extensiones de clave que proporcionan un mínimo de 112 bits de solidez efectiva de clave y prácticas adecuadas de administración de claves. La criptografía es un método de protección de datos e incluye tanto cifrado (que es reversible) como hashing (que es de un solo uso; es decir, no reversible). Ver *Hashing.* Al momento de la publicación, algunos ejemplos de normas y algoritmos de cifrado probados y aceptados por la industria incluyen: AES (128 bits y superior), TDES/TDEA (claves de triple extensión), RSA (2048 bits y superior), ECC (224 bits y superior) y DSA/D-H (2048/224 bits y superior). Para obtener más información respecto de la solidez de las claves criptográficas y sobre los algoritmos, consulte la versión actual de NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/). ***Nota:*** *Los ejemplos anteriores son apropiados para el continuo almacenamiento de datos de titulares de tarjeta. Los requisitos mínimos criptográficos para operaciones basadas en transacciones, tal como se define en PCI PIN y PTS, son más flexibles debido a que hay controles adicionales instalados para reducir el nivel de exposición.* *Se recomienda que todas las implementaciones nuevas utilicen un mínimo de 128 bits de solidez efectiva de clave.*

Término	Definición
SysAdmin	Abreviatura de “system administrator” (administrador de sistemas). Persona con alto nivel de privilegios responsable de administrar un sistema informático o una red.
Componentes del sistema	Todo componente de red, servidor, dispositivo informático o aplicación que se incluye en el entorno de datos del titular de la tarjeta o está conectado a él.
Objeto de nivel de sistema	Cualquier cosa en un componente del sistema que se requiere para su operación, incluyendo, pero sin limitarse a, tablas de bases de datos, procedimientos almacenados, archivos ejecutables y de configuración de la aplicación, archivos de configuración del sistema, bibliotecas estáticas y compartidas y DLL, ejecutables del sistema, controladores de dispositivos y archivos de configuración de dispositivos, y componentes de terceros.
TACACS	Acrónimo de “terminal access controller access control system” (sistema de control de acceso del controlador de acceso a terminales). Protocolo de autenticación remoto que se utiliza generalmente en redes que se comunican entre un servidor de acceso remoto y un servidor de autenticación para determinar los derechos de acceso del usuario a la red. Este método de autenticación se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de múltiples factores.
TCP	Acrónimo de “Transmission Control Protocol” (protocolo de control de transmisión). Uno de los protocolos de capa de transporte centrales del conjunto de Protocolo de Internet (IP), y el lenguaje comunicativo o protocolo básico de Internet. Consulte *IP*.
TDES	Acrónimo de “Triple Data Encryption Standard” (Estándar de cifrado de datos triple), también denominado “3DES” o “Triple DES”. Cifrado por bloques formado por un cifrado DES repetido tres veces. Consulte *Criptografía sólida.*
TELNET	Abreviatura de “telephone network protocol” (protocolo de redes telefónicas). En general, se utiliza para proporcionar sesiones de inicio con líneas comandos orientadas al usuario para dispositivos de red. Las credenciales del usuario se transmiten en texto simple.
Amenaza	Condición o actividad capaz de ocasionar que, intencional o accidentalmente, la información o recursos para el procesamiento de la información se pierdan, modifiquen, queden expuestos o vuelvan inaccesibles; o que sean afectados de algún otro modo en detrimento de la organización.
TLS	Acrónimo de “transport layer security” (seguridad de capa de transporte). Diseñado para brindar integridad y confidencialidad de datos en la comunicación entre dos aplicaciones. TLS es el sucesor de SSL.
Token	En el contexto de las autenticaciones y del control de acceso, un token es un valor proporcionado por un hardware o software que suele funcionar con un servidor de autenticación o VPN para realizar autenticaciones dinámicas o de múltiples factores. Consulte *RADIUS, TACACS* y *VPN.* Ver también *Token de sesión*.

Término	Definición
Datos de la pista.	También denominados “contenido completo de la pista” o “datos de la banda magnética” Datos codificados en la banda magnética o el chip que se utilizan para la autenticación y/o autorización durante las transacciones de pago. Puede ser la imagen de la banda magnética de un chip o los datos de la pista 1 y/o pista 2 de la banda magnética.
Datos de transacciones	Datos relacionados a las transacciones con tarjetas de pago electrónico.
Troyano	También denominado “caballo de Troya”. Una clase de software malicioso que al instalarse permite al usuario ejecutar funciones normalmente, mientras los troyanos ejecutan funciones maliciosas sin que este lo sepa.
Truncamiento	Método mediante el cual se elimina definitivamente un segmento de datos del PAN, con lo cual todo el PAN se vuelve ilegible. El truncamiento se relaciona con la protección de PAN cuando *se almacena* en archivos, bases de datos, etc. Vea *Ocultamiento* para la protección de PAN cuando *se muestra* en pantallas, recibos de papel, etc.
Red de confianza	Red de una organización que la empresa es capaz de controlar o administrar.
Red no confiable	Red que se encuentra afuera de las redes de una organización y que, por ende, la empresa no puede controlar o administrar.
URL	Acrónimo de “Uniform Resource Locator” (localizador uniforme de recursos).Una cadena de texto con formato que utilizan los exploradores web, los clientes de correo electrónico y otro tipo de software para identificar un recurso de red en Internet.
Metodología de control de versiones	Un proceso mediante el cual se asignan esquemas de versiones para identificar en forma única un estado particular de una aplicación o un software. Estos esquemas respetan un formato de número de versión, uso de número de versión y cualquier elemento comodín según lo define el proveedor de software. Los números de versión suelen asignarse en orden ascendente y corresponden a un cambio particular en el software.
Dispositivo virtual (VA)	Un VA toma el concepto de un dispositivo preconfigurado para realizar un conjunto específico de funciones y ejecuta este dispositivo como una carga de trabajo. Generalmente, un dispositivo de red existente se virtualiza para ejecutarse como un dispositivo virtual, como un router, conmutador o firewall.
Hipervisor virtual	Consulte *Hipervisor***.**
Máquina virtual	Entorno operativo independiente que se comporta como una computadora separada. También se conoce como “huésped”, y se ejecuta por encima de un hipervisor.
Supervisor de máquinas virtuales (VMM)	El VMM está incluido con el hipervisor y es un software que implementa abstracción de hardware de máquinas virtuales. Administra el procesador, la memoria y otros recursos del sistema para asignar lo que cada sistema operativo huésped requiere.

Término	Definición
Terminal de pago virtual	Un terminal de pago virtual es un acceso basado en explorador web para un adquiriente, procesador o sitio web de proveedor de servicios externos que permite autorizar transacciones de tarjetas de pago, donde el comerciante ingresa manualmente datos de tarjetas de pago mediante un explorador web conectado de forma segura. A diferencia de los terminales físicos, los terminales de pago virtuales no leen datos directamente de una tarjeta de pago. 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.
Conmutador virtual o router	Un conmutador virtual o router es una entidad lógica que presenta funciones de ruteo y conmutación de datos a nivel de la infraestructura. Un conmutador virtual es parte integral de una plataforma de servidores virtualizada, como un controlador, módulo o complemento hipervisor.
Virtualización	La virtualización se refiere a la abstracción lógica de recursos informáticos a partir de restricciones físicas. Una abstracción común es la denominada máquina virtual o VM, la cual toma el contenido de una máquina física y permite operar en hardware físico diferente y/o junto con otras máquinas virtuales en el mismo hardware físico. Además de las VM, la virtualización se puede realizar en muchos otros recursos informáticos, incluyendo aplicaciones, escritorios, redes y almacenamiento.
VLAN	Abreviatura de “virtual LAN” (LAN virtual) o “virtual local area network” (red de área local virtual). Red de área local lógica que se extiende más allá de una sola red física de área local.
VPN	Acrónimo de “virtual private network” (red privada virtual). Una red informática donde algunas conexiones son circuitos virtuales dentro de redes más extensas, como Internet, en lugar de conexiones directas por medio de cables físicos. Cuando este es caso, los puntos finales de una red virtual se transmiten a través de una red mayor. Al contrario de una aplicación común, formada por comunicaciones seguras en la red pública, una red VPN puede presentar o no funciones de seguridad, como la autenticación y el cifrado de contenidos. Una VPN se puede utilizar con un token, tarjeta inteligente, etc., para proporcionar autenticación de dos factores.
Vulnerabilidad	Error o debilidad que, de llegar a explotarse, puede ocasionar una exposición a riesgos del sistema, intencionalmente o no.
WAN	Acrónimo de “wide area network” (red de área amplia). Red informática que abarca un área amplia, a menudo parte de un sistema con cobertura en toda una región o empresa.
Aplicación web	Una aplicación a la que generalmente se accede mediante un explorador web o a través de servicios web. Las aplicaciones web pueden estar disponibles a través de Internet o en una red privada e interna.
Servidor web	Computadora con un programa capaz de aceptar pedidos HTTP de clientes web y brindar respuestas HTTP (en general, páginas web).

Término	Definición
WEP	Acrónimo de “wired equivalent privacy” (privacidad equivalente por cable). Algoritmo débil utilizado en el cifrado de redes inalámbricas. Expertos de la industria han informado que la conexión WEP presenta varias debilidades tan serias que puede descifrarse en minutos utilizando herramientas de software comunes. Consulte *WPA.*
Comodín	Carácter que puede sustituirse con un subconjunto definido de posibles caracteres en un esquema de versión de una aplicación. En el contexto de las PA-DSS, los caracteres comodines se pueden utilizar, opcionalmente, para representar varios cambios que no afecten la seguridad. Un elemento comodín es el único elemento variable del esquema de la versión del proveedor y se utiliza para indicar que los cambios representados por el elemento comodín son secundarios y no afectan la seguridad entre cada versión.
Punto de acceso cámbrico	También denominado “AP”. Dispositivo que permite a los mecanismos de comunicación inalámbrica conectarse a una red inalámbrica. Usualmente conectado a una red con cable, es capaz de transferir por medio de la red datos entre dispositivos inalámbricos y con cable.
Redes inalámbricas	Red que conecta computadoras sin necesidad de una conexión física de cables.
WLAN	Acrónimo de “wireless local area network” (red de área local inalámbrica). Red de área local que se conecta a dos o más computadoras o dispositivos sin cables.
WPA/WPA2	Acrónimo de “WiFi Protected Access” (acceso protegido WiFi). Protocolo de seguridad creado para asegurar las redes inalámbricas. WPA es la tecnología sucesora de WEP. También se lanzó WPA2, tecnología sucesora de WPA.