PCI Security Standards Council®

Guía Rápida de Referencia de PCI DSS v4.0

Comprensión de la versión 4.0 del Estándar de Seguridad de Datos de Payment Card Industry

Para los comerciantes y las demás entidades involucradas en el procesamiento de datos de las cuentas de pago

Contenidos

Guía Rápida de Referencia de PCI DSS: Comprensión de la versión 4.0 del Estándar de Seguridad de Datos de Payment Card Industry.

Esta Guía Rápida de Referencia del Estándar de Seguridad de Datos PCI (PCI DSS) es proporcionada por PCI Security Standards Council (PCI SSC) para informar y educar a los comerciantes y a las demás entidades involucradas en el procesamiento de tarjetas de pago. Para más información en relación a PCI SSC y a los estándares que gestionamos, visite https://pcisecuritystandards.org.

El propósito de este documento es proporcionar información complementaria, la cual no sustituye ni reemplaza los estándares PCI o sus documentos de respaldo.

Agosto de 2022

Contenidos

La Importancia de Proteger los Datos de las Cuentas de Pago con el Estándar de Seguridad de Datos PCI 4

Información General de los Estándares de PCI SSC 6

Introducción a PCI DSS 8

- Información sobre la Aplicabilidad de PCI DSS 9
- El Rol de PCI SSC y las Marcas de Pago Participantes 11
- Los Profesionales de Asistencia con las Evaluaciones de PCI DSS 11
- Informes de Resultados de las Evaluaciones de PCI DSS 12
- Elección de un Asesor de Seguridad Calificado 13
- Elección de un Proveedor de Análisis Aprobado 14
- Proceso de Evaluación de PCI DSS 14
- Alcance de los Requisitos de PCI DSS 15
- Uso de Proveedores de Servicios Externos (TPSP) 16
- Implementación de PCI DSS en los Procesos de BAU 18

Comprensión de PCI DSS v4.0 20

- Enfoques para Implementar y Validar PCI DSS 20
- Comprensión de la Estructura y el Contenido de los Requisitos de PCI DSS 23
- Resumen de los Requisitos, del 1 al 12, de PCI DSS v4.0 23

Recursos 35

Acerca de PCI Security Standards Council 37

Esta Guía proporciona información complementaria que no sustituye ni reemplaza los Estándares de Seguridad PCI SSC o sus documentos de respaldo.

La Importancia de Proteger los Datos de las Cuentas de Pago con el Estándar de Seguridad de Datos PCI

La aceleración global de las transacciones que se realizan sin dinero en efectivo colocan a los sistemas de pago en la mira de los criminales que buscan ganar dinero fácil. Los datos de las cuentas de pago son su atracción Número Uno, el 84 % de los casos de fuga de datos implicó a los datos de tarjetas de pago, de acuerdo a Verizon. Todos ellos buscan el camino más simple para robar los datos de las cuentas de pago que utilizan las tarjetas de pago y los sistemas de pago electrónico relacionados.

Como parte interesada del sistema de pago, su compañía está en la primera linea de defensa en una batalla de alto riesgo por mantener la seguridad de los datos de pago contra el robo y el aprovechamiento. Una seguridad laxa ocasional permite a los criminales robar y utilizar la información financiera personal del consumidor de las transacciones de pago o de los sistemas de procesamiento.

Las vulnerabilidades pueden aparecer en cualquier parte del ecosistema de procesamiento de tarjetas, incluidos, entre otros:

- dispositivos en puntos de venta;
- sistemas con base en la nube;
- dispositivos móviles, computadoras o servidores personales;
- puntos de acceso inalámbrico;
- aplicaciones para compras en línea;
- sistemas de almacenamiento en formato impreso;
- la transmisión de los datos del tarjehabientes a los proveedores de servicios;
- conexiones de acceso remoto.

Las vulnerabilidades también pueden extenderse a los sistemas operados por los proveedores de servicios y los adquirentes, que son las instituciones financieras que inician y mantienen las relaciones con los comerciantes que aceptan tarjetas de pago (ver gráfico en la página 5).

El cumplimiento de PCI DSS contribuye a reducir estas vulnerabilidades y a proteger los datos de las cuentas de pago.

Esta Guía proporciona información complementaria que no sustituye ni reemplaza los Estándares de Seguridad PCI SSC o sus documentos de respaldo.

ATRACCIÓN N.°1 SON LOS DATOS DE LAS CUENTAS DE PAGO

84 % de los casos de fuga de datos implicó a los datos de las cuentas de pago.

93 % de las fugas de datos fueron cometidas por motivos económicos.

Fuente: Verizon 2022 *Data Breach Investigations Report*, páginas 18 y 25. https://www.verizon.com/business/resources/reports/dbir/

El propósito de esta Guía Rápida de Referencia de PCI DSS v4.0 es ayudarlo a comprender cómo es que PCI DSS protege su entorno de procesamiento de pagos y cómo aplicar el Estándar.

Hay cuatro pasos recurrentes para proteger los datos de las cuentas de pago con PCI DSS:

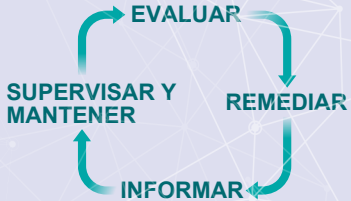
Evaluar – identificar todas las ubicaciones de los datos de las cuentas de pago, hacer un inventario de todos los activos de IT y de los procesos de negocios vinculados con el procesamiento de pago, analizarlos en busca de vulnerabilidades que pudieran exponer los datos de cuentas de pago, implementar y actualizar los controles necesarios y realizar una evaluación formal de PCI DSS.

Remediar – identificar y solucionar cualquier vacío en los controles de seguridad, resolver las vulnerabilidades identificadas, remover con seguridad cualquier almacenamiento innecesario de datos de pago e implementar procesos de negocios seguros.

Informar – documentar los detalles de las evaluaciones y las soluciones, y presentar informes de cumplimiento a la entidad receptora de cumplimientos (generalmente, el banco adquirente o las marcas de pago).

Supervisar y Mantener – confirmar que los controles de seguridad están implementados para asegurar que los datos de las cuentas de pago y el entorno continúen funcionando de manera efectiva y adecuada a lo largo del año. Estos procesos de «negocios habituales» deberán implementarse como parte de la estrategia de seguridad integral de la entidad para asegurar la protección de forma permanente.

PCI DSS ES UN PROCESO CONTINUO



Esta Guía proporciona información complementaria que no sustituye ni reemplaza los Estándares de Seguridad PCI SSC o sus documentos de respaldo.

Información General de los Estándares de PCI SSC

Los Estándares de Seguridad PCI mejoran la seguridad de pagos con requisitos de control de seguridad sólidos e integrales, procedimientos de evaluación y materiales de apoyo. Los estándares definen los controles de seguridad y los procesos para las entidades involucradas con el ecosistema de pagos, así como los requisitos para los desarrolladores y los proveedores de soluciones, para construir y asegurar los dispositivos de gestión de pagos, el *software* y las soluciones para la industria de pagos.

Más abajo se proporciona una descripción de los Estándares PCI. Algunos de estos estándares resultan en dispositivos de pago validados por una lista de PCI, en *software* o en soluciones que pueden utilizarse junto a PCI DSS para asegurar los entornos de los datos de pago.

El Estándar de Seguridad de Datos PCI – Un marco ejecutable para el desarrollo de procesos robustos de seguridad de datos de las cuentas de pago, incluidas la prevención, detección y reacción adecuada a los incidentes de seguridad.

PIN de Seguridad de Transacción (PTS) – Los requisitos de seguridad que se enfocan en las características y el manejo de dispositivos utilizados en la protección de los PIN de los titulares de la tarjeta (números de identificación personales) y otros datos sensibles de pago. El estándar del Punto de Interacción PTS (POI) cubre los dispositivos que incluyen las terminales PIN, los dispositivos de POS (puntos de venta), las plataformas de cifrado de PIN y las terminales de pago sin atención. El estándar del Módulo de Seguridad del Hardware de PTS (HSM) define los requisitos de seguridad para HSM, para asegurar la confidencialidad y la integridad de los datos durante actividades tales como las transacciones financieras y la personalización de la tarjeta de pago.

Marco de Seguridad del Software – Un grupo de estándares y programas para asegurar el diseño, el desarrollo y el mantenimiento del *software* de pago existente y del futuro. Incluye el Estándar del Ciclo Vital del Software Seguro (SLC Seguro) y el Estándar del *Software* Seguro.

Soluciones Cifrado Punto por Punto (P2PE) – Un sistema integral de requisitos de seguridad para las soluciones de validación P2PE, para proteger los datos de las cuentas de pago a través de un cifrado en donde se recogen, en la terminal de pago, hasta su descifrado en el entorno del proveedor de soluciones.

Los Estándares de Seguridad PCI se desarrollan y se mantienen por PCI Security Standards Council y las partes interesadas de la industria de tarjetas de pago global.

Los Estándares de Móviles – Incluye el estándar de Pagos sin Contacto en COTS (CPoC) y el estándar del Ingreso con PIN en COTS basado en Software (SPoC) para soluciones que aceptan los pagos móviles en dispositivos comerciales fuera de la plataforma (COTS) (por ejemplo teléfonos inteligentes o tabletas), en un entorno atendido por comerciantes.

Otros Estándares – Otros Estándares de PCI definen los controles y los requisitos de prueba para la seguridad de PIN, la producción y provisión de tarjetas físicas y lógicas, los proveedores de servicios de token y el acceso de seguridad (3-D Seguro).

Los Estándares PCI pueden descargarse de la Biblioteca Documental de PCI SSC:
https://pcisecuritystandards.org/document_library

Introducción a PCI DSS

PCI DSS se desarrolló para fomentar y mejorar la seguridad de los datos de las cuentas de pago y para facilitar la adopción generalizada de medidas de seguridad de datos consistentes, a nivel mundial. PCI DSS proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos de las cuentas de pago.

Objetivos	Requisitos de PCI DSS
Construir y Mantener Redes y Sistemas Protegidos	1. Instalar y mantener los controles de seguridad de la red 2. Aplicar configuraciones deguras a todos los componentes del sistema
Proteger los Datos del Tarjetahabiente	3. Proteger los datos de tarjetahabientes almacenados 4. Proteger los datos de tarjetahabientes con criptografía robusta durante la transmisión a través de redes abiertas y publicas
Mantener un Programa de Gestión de Vulnerabilidades	5. Proteger todos los sistemas y redes de software malicioso 6. Desarrollar y mantener sistemas y softwares seguros
Implementar Medidas Sólidas de Control de Acceso	7. Restringir el acceso a los componentes del sistema y a los datos de tarjetahabientes según la necesidad de conocimiento de la Empresa 8. Identificar a los usuarios y autenticar el acceso a los componentes del sistema 9. Restringir el acceso físico a los datos de tarjetahabientes
Monitorear y Verificar las Redes Regularmente	10. Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabientes 11. Poner a prueba regularmente la seguridad de los sistemas y de las redes
Mantener una Política de Protección Informática	12. Respaldar la seguridad de la información con políticas y programas organizacionales

PCI DSS PROTEGE MÁS QUE LOS DATOS DE LAS CUENTAS DE PAGO

Si bien está diseñado específicamente para enfocarse en entornos con datos de las cuentas de tarjetas de pago, PCI DSS también se puede utilizar como protección ante amenazas y para asegurar los demás elementos en el ecosistema de pagos.

Información de Aplicabilidad PCI DSS

Los PCI DSS están destinados a todas las entidades que almacenan, procesan o transmiten datos de tarjetahabientes (CHD) y/o datos de autenticación sensibles (SAD) o que podrían afectar la seguridad del entorno de datos de tarjetahabientes (CDE). Esto incluye a todas las entidades involucradas en el procesamiento de cuentas de tarjetas de pago, incluidos los comerciantes, procesadores, adquirentes, emisores y otros proveedores de servicios. Los datos del tarjehabientes y los datos sensibles de autenticación se consideran datos de las cuentas y se definen de la siguiente manera:

Datos de Tarjetahabientes	
Los Datos de Tarjetahabientes incluyen:	**Los Datos Sensibles de Autenticación incluyen:**
• Número de Cuenta Principal (PAN) • Nombre del Tarjetahabiente • Fecha de Expiración • Código de Servicio	• Datos de pista completos (datos de banda magnética o equivalentes en un chip) • Código de verificación de la tarjeta • PIN / bloques de PIN

Los requisitos de PCI DSS se aplican a las entidades con entornos donde los datos de las cuentas (datos del tarjehabientes o datos sensibles de autenticación) se almacenan, procesan o transmiten, y entidades con entornos que puedan afectar la seguridad del CDE. Algunos requisitos de PCI DSS también pueden a entidades con entornos que no almacenan, procesan ni transmiten datos de las cuentas, por ejemplo, a entidades que subcontratan operaciones de pago o la administración de su CDE.

El número de cuenta principal (PAN) es el factor que define los datos de trajetahabientes. El término «datos de trajetahabientes» involucra lo siguiente: el PAN completo, cualquier otro elemento de los datos de datos de trajetahabientes que estén presente en el PAN y cualquier elemento de los datos sensibles de autenticación.

Si el nombre del trajetahabiente, el código de servicio y/o la fecha de caducidad se almacenan, procesan o transmiten con los datos PAN, o están presentes presentes en el CDE, estos deben estar protegidos de acuerdo con los requisitos PCI DSS aplicables a los datos de trajetahabientes.

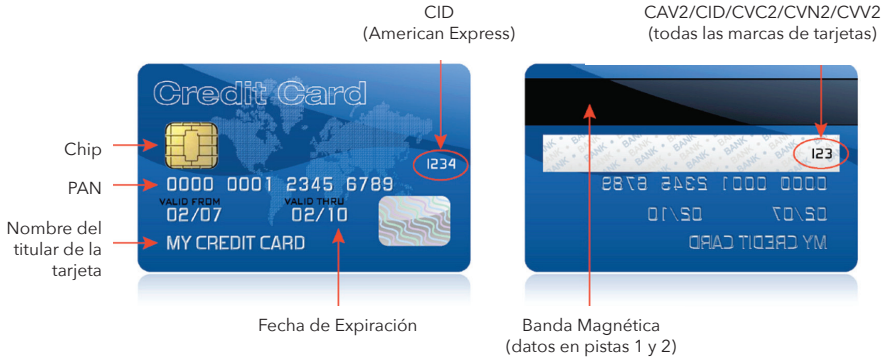
TERCERIZACIÓN DE LA PROTECCIÓN DE LOS DATOS DE LAS CUENTAS

Las entidades que subcontratan sus entornos de pago u operaciones de pago a terceros siguen siendo responsables de garantizar que los datos de las cuentas estén protegidos por el tercero de acuerdo con los requisitos aplicables de PCI DSS.

Si una entidad almacena, procesa o transmite datos PAN, entonces existe un CDE al que se le aplicarán los requisitos de PCI DSS. Algunos requisitos pueden no ser aplicables, por ejemplo, si la entidad no almacena datos PAN, entonces los requisitos relacionados con la protección del datos PAN almacenados, en el Requisito 3, no serán aplicables a la entidad.

El siguiente gráfico muestra en qué lugar de la tarjeta de pago se encuentra la información ilustrada en la tabla anterior. Estos elementos de los datos de las cuentas dispuestos en tarjetas de pago físicas también se encuentran en los dispositivos con funcionalidades que emulan un pago con tarjeta, tales como un token de pago en un dispositivo móvil o en un reloj inteligente.

Tipos de Datos en una Tarjeta de Pago



El Rol de PCI SSC y las Marcas de Pago Participantes

PCI SSC es el responsable de desarrollar y administrar los Estándares de Seguridad PCI y los programas de calificación y de publicación relacionados; sin embargo, cada Marca de Pago Participante mantiene sus propios programas de observancia de cumplimientos, que incluyen qué entidades necesitan validar cumplimientos, los niveles de validación, si una entidad es elegible para completar el Cuestionario de Autoevaluación (SAQ) o si debe completar un Informe de Cumplimiento (ROC), así como la imposición de cualquier multa o penalidad.

¿Preguntas? Las preguntas relacionadas con los programas de cumplimiento de las marcas de pago, incluidas las de cómo informar los resultados de las evaluaciones de PCI DSS y las que son para comprender cualquier requisito adicional que puedan especificar las marcas de pago, deben dirigirse a su adquirente o a las marcas de pago directamente. Los detalles de contacto de las marcas de pago se pueden encontrar en la FAQ 1142 «¿cómo contactar a las marcas de tarjetas de pago?» en el sitio web de PCI SSC.

Los Profesionales de Asistencia con las Evaluaciones de PCI DSS

PCI SSC administra varios programas que califican a los profesionales de la industria para facilitar el proceso de evaluación de PCI DSS.

Asesores de Seguridad Calificados. Los Asesores de Seguridad Calificados (QSA) son organizaciones de seguridad independientes que han sido calificadas por PCI SSC para asesorar y validar la adhesión de la entidad a PCI DSS.

Asesores de Seguridad Interna. El programa de Asesores de Seguridad Interna (ISA) proporciona una oportunidad para los empleados de las compañías, que patrocinan a los ISA calificados de PCI, de recibir entrenamiento y calificación para mejorar el entendimiento de los empleados de PCI DSS, facilitar las interacciones de la entidad con los QSA, aumentar la calidad, la confiabilidad y la consistencia de las autoevaluaciones de la entidad y apoyar la aplicación constante y adecuada de los controles y medidas de PCI DSS.

Proveedores de Análisis Aprobados. Los Proveedores de Análisis Aprobados (ASV) están calificados por PCI SSC para proporcionar un sistema de servicios y herramientas de seguridad (solución de análisis ASV) para realizar los servicios de análisis de vulnerabilidad externos a fin de validar la adhesión a los requerimientos de análisis de vulnerabilidad externo de PCI DSS.

Los Profesionales de Payment Card Industry. El programa de Profesionales de Payment Card Industry (PCIP) proporciona una acreditación básica para los profesionales de la industria que demuestren su conocimiento y su comprensión profesional de los estándares PCI SSC y de los materiales de respaldo.

La FAQ 1142 se encuentra disponible en: https://pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/

INTEGRADORES Y REVENDEDORES CALIFICADOS (QIR)

Los Integradores y Revendedores Calificados (QIR) son integradores y revendedores especialmente capacitados por PCI Security Standards Council para gestionar los controles de seguridad críticos al instalar los sistemas de pagos de los comerciantes. Los QIR reducen el riesgo del comerciante y mitigan las causas más comunes de las fugas de los datos de pagos al enfocarse en los controles de seguridad críticos.

Se pueden encontrar detalles adicionales y el listado de asesores y soluciones en el sitio web de PCI SSC en: https://www.pcisecuritystandards.org/program-listings-overview/

Informes de Resultados de las Evaluaciones de PCI DSS

Los documentos de validación son el mecanismo oficial por medio del cual las entidades transmiten su estatus de cumplimiento de PCI DSS a su adquirente o a las marcas de pago. Dependiendo de los programas de cumplimiento de las marcas de pago, se puede requerir a las entidades que superen una evaluación detallada de PCI DSS y presenten un Informe sobre Cumplimiento, o que sean elegibles para realizar una autoevaluación y presentar un Cuestionario de Autoevaluación. Una Atestación de Cumplimiento, firmada por la entidad y el QSA (si hubo) debe acompañar el documento de validación. Puede requerirse también la presentación cuatrimestral de un informe de análisis ASV para analizar las vulnerabilidades en la red.

Informe de Cumplimiento. El Informe de Cumplimiento (ROC) es un informe detallado para que los asesores documenten los resultados de una evaluación de PCI DSS. EL ROC contiene información más detallada que los Cuestionarios de Autoevaluación, incluida la información sobre el entorno de la entidad, las muestras que el asesor ha seleccionado y cómo se evaluó y validó cada requisito. La Plantilla de ROC proporciona instrucciones de informes detallados para los asesores y es obligatorio para que utilicen los QSA en cualquier evaluación de PCI DSS que se documenta en el ROC.

Cuestionarios de Autoevaluación. Los Cuestionarios de Autoevaluación (SAQ) proporcionan herramientas de validación alternativas para entidades que, de acuerdo a los programas de cumplimiento de las marcas de pago, son aptas para realizar autoevaluaciones que validen su cumplimiento de PCI DSS y que cumplen con el Criterio de Elegibilidad de SAQ especificado en cada SAQ. Distintos SAQ se encuentran disponibles para los diferentes entornos de los comerciantes, incluidos los entornos de comercio electrónico y el entorno de las soluciones de Cifrado de Punto a Punto (P2PE) de la lista de PCI. La mayoría de los SAQ incluyen un subgrupo de aquellos requisitos de PCI DSS que solo son aplicables a un entorno particular. Pueden encontrarse más detalles en el documento de Instrucciones y Directrices de SAQ y en la sección SAQ del sitio web de PCI SSC. Para determinar si usted es elegible para completar un SAQ y, en caso positivo, cuál sería el SAQ adecuado, contacte con las marcas de pago o su banco adquirente.

Atestaciones de Cumplimiento. Una Atestación de Cumplimiento (AOC) es una declaración de los resultados de una evaluación de PCI DSS, completada y firmada por la entidad que fue evaluada y el QSA de la compañía (si hubo). La AOC refleja los resultados de la evaluación de PCI DSS que se documentan en un ROC vinculado o SAQ.

ENFOQUE PRIORIZADO

PCI SSC también proporciona el Enfoque Priorizado de PCI DSS para que las partes interesadas entiendan cómo reducir el riesgo de forma anticipada en su recorrido por PCI DSS. El Enfoque Priorizado distribuye todos los requisitos de PCI DSS en seis objetivos de seguridad basados en riesgos y proporciona una herramienta que pueden utilizar las entidades para rastrear su progreso a medida que cumplen los requisitos de PCI DSS. Esto los ayuda a protegerse de manera progresiva contra los factores de mayor riesgo primero, mientras los acerca al cumplimiento de PCI DSS.

PROVEEDOR DE SERVICIO SAQ

Cuestionario de Autoevaluación D para Proveedores de Servicios es el **ÚNICO SAQ,** para los proveedores de servicios.

PROVEEDOR DE SERVICIO AOC

Si un proveedor de servicios dispone de una Atestación de Cumplimiento (AOC) se espera que proporcione el AOC a los clientes que lo soliciten.

Elección de un Evaluador de Seguridad Calificado

Durante la evaluación de PCI DSS los QSA se encargan de:

- Verificar toda la información técnica proporcionada por el comerciante al proveedor de servicios
- Utilizar un criterio objetivo para determinar si el estándar se cumplió
- Proporcionar soporte y guía durante el proceso de cumplimiento
- Cumplir los Requisitos de PCI DSS y los Procedimientos de Prueba
- Validar el alcance de la evaluación
- Evaluar los controles compensatorios y las implementaciones del enfoque personalizado
- Elaborar el informe final

El QSA que elija deberá tener sólidos conocimientos de su negocio y contar con experiencia en el asesoramiento de seguridad de otros negocios similares. Dichos conocimientos permiten que el QSA entienda los distintos matices del sector de su negocio cuando asegure los datos de pago de acuerdo a PCI DSS. También, es recomendable que se ajuste a la cultura de su compañía. Mientras que la evaluación concluirá, independientemente de que se cumplan o no los requisitos de PCI DSS, los QSA pueden prestar apoyo más allá de la evaluación, al trabajar con su organización para ayudarlo a comprender cómo lograr y mantener el cumplimiento de forma continua. Muchos QSA pueden proporcionar servicios adicionales relacionados con la seguridad, tales como realizar evaluaciones de vulnerabilidad periódicas y dar soluciones. Una lista de QSA se encuentra disponible en https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

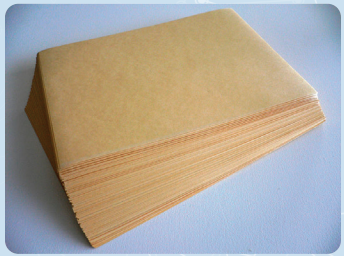
Elección de un Proveedor de Análisis Aprobado

El ASV se encarga de determinar si el cliente cumple los requisitos de análisis de vulnerabilidades externas de PCI DSS. Los ASV y sus soluciones de análisis ASV están calificadas por PCI Security Standards Council para realizar los análisis de redes externas y de los sistemas que requiere PCI DSS. Un ASV puede utilizar su propio *software* o una solución de fuente abierta comercial aprobada por PCI como parte del proceso de calificación del ASV. Una solución de análisis del ASV incluye los procedimientos de análisis y las herramientas, los informes de análisis vinculados y el proceso de intercambio de información entre el proveedor de análisis y el cliente del mismo. Los ASV pueden presentar un informe de análisis de ASV a la institución adquirente en beneficio del comerciante o del cliente del proveedor de servicios, si así fuera acordado por el ASV y su cliente. Más información acerca de los ASV y sus soluciones de análisis, de las obligaciones de los clientes de los análisis y sobre los requisitos de análisis de vulnerabilidades externas de PCI DSS pueden encontrarse en la Guía del Programa de ASV en el sitio web de PCI SSC. Una lista de ASV se encuentra disponible en https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

Proceso de Evaluación de PCI DSS

El proceso de evaluación de PCI DSS incluye los siguientes pasos de alto nivel:

1. **Alcance** – determinar en dónde se almacenan, procesan y transmiten los datos de las cuentas de pago, así como qué sistemas y redes se encuentran dentro del alcance de PCI DSS y confirmar el alcance de la evaluación.
2. **Evaluar** – realizar la evaluación respecto a todos los componentes del sistema alcanzados, para determinar si se cumplen los requisitos de PCI DSS, mediante el seguimiento de los procedimientos de prueba para cada requisito de PCI DSS.
3. **Informar** – completar la documentación requerida (por ejemplo, el Cuestionario de Autoevaluación [SAQ] o el Informe de Cumplimiento [ROC]), incluida la documentación de todos los controles compensatorios y de cualquier otro requisito que se cumple con el enfoque personalizado.
4. **Atestar** – completar la Atestación de Cumplimiento (AOC) correspondiente, en su totalidad. Las AOC solo están disponibles en el sitio web de PCI SSC.



Reunir Documentación: Las políticas de seguridad, los registros de cambio de control, los esquemas de redes, los informes de análisis, los documentos del sistema, los registros de entrenamientos y demás documentos.

Programar los Recursos: Garantizar la participación de los altos ejecutivos, así como la de los directores de proyectos y de las personas clave de TI, de seguridad, de las aplicaciones, de recursos humanos y del área legal.

Describir el Entorno: Organizar la información sobre el entorno de los titulares de las tarjetas, incluidos los flujos de los datos de las cuentas y las ubicaciones de los repositorios de los datos de las cuentas.

Foto: Wikimedia Commons

5. **Presentar** – presentar la documentación correspondiente de PCI SSC (SAQ o ROC) y la AOC, junto con cualquier otra documentación de respaldo solicitada, como son los informes de análisis de ASV a la entidad solicitante (aquellas que administran los programas de cumplimiento, tales como las marcas de pago y los adquirentes [para los comerciantes] o a los demás solicitantes [para los proveedores de servicios]).
6. **Solucionar** – si es necesario, realizar correcciones para atender los requisitos que no se hayan cumplido y proporcionar un informe actualizado.

Alcance de los Requisitos de PCI DSS

Los requisitos de PCI DSS se aplican a:

- El entorno de los datos del tarjehabientes (CDE) se compone de:
  - Los componentes del sistema, las personas y los procesos que almacenan, procesan y transmiten los datos del tarjehabientes o los datos sensibles de autenticación; y,
  - los componentes del sistema que pueden no almacenar, procesar o transmitir CHD/SAD, pero que tienen una conectividad sin restricciones con los componentes del sistema que almacenan, procesan o transmiten CHD/SAD.

Y

- los componentes del sistema, las personas y los procesos que podrían afectar la seguridad del CDE.

Los «componentes del sistema» incluyen los dispositivos de red, los servidores, los dispositivos informáticos, los componentes virtuales, los componentes de la nube y el *software*. Visite la sección «Alcance los Requisitos de PCI DSS» en PCI DSS para ver ejemplos de los «componentes del sistema».

Confirmación Anual del Alcance de PCI DSS

El primer paso para prepararse para una evaluación de PCI DSS es que la entidad evaluada determine con precisión el alcance de la revisión. La entidad evaluada debe confirmar la precisión del alcance de PCI DSS, de acuerdo con el Requisito 12.5.2 de PCI DSS, al identificar todas las ubicaciones y flujos de datos de la cuenta y todos los sistemas que están conectados o, si estuvieran comprometidos, que pudieran afectar el CDE (por ejemplo, los servidores de autenticación, los servidores de acceso remoto o los servidores de registro), para garantizar que estén incluidos en el alcance de PCI DSS. Se deben considerar todos los sistemas y todas las ubicaciones durante proceso de determinación de alcance, incluidos los sitios de respaldo/recuperación y los sistemas de conmutación por error.

CONFIRMACIÓN ANUAL DEL ALCANCE DE PCI DSS

Esta confirmación anual del alcance de PCI DSS se define en el Requisito 12.5.2 de PCI DSS y se espera que sea realizada por la entidad. Esta actividad no es la misma que, ni se pretende que sea reemplazada por, la confirmación del análisis inicial realizada por el asesor de la entidad durante la evaluación.

Los pasos mínimos para que una entidad confirme la precisión del alcance de PCI DSS se especifican en el Requisito 12.5.2 de PCI DSS. Se espera que la entidad retenga la documentación para mostrar cómo se determinó el alcance de PCI DSS. La documentación se conserva para la revisión del asesor y como referencia durante la próxima actividad de confirmación del alcance de PCI DSS de la entidad. Para cada evaluación de PCI DSS, el asesor validará que la entidad definió y documentó con precisión el alcance de la evaluación.

Segmentación

Se puede reducir el alcance de la evaluación de PCI DSS con el uso de segmentación, que separa el entorno de los datos de los titular de las tarjetas de las demás conexiones de una entidad. La reducción del alcance puede disminuir el costo de la evaluación de PCI DSS, reducir el costo y la dificultad de implementar y mantener los controles de PCI DSS, así como el riesgo para la entidad. Para que se considere fuera del alcance de PCI DSS, el componente del sistema debe estar segmentado (aislado) correctamente del CDE, de forma tal que el componente del sistema que está fuera de alcance no pueda afectar la seguridad del CDE, incluso si ese componente se vio comprometido. Visite la sección «Segmentación» de PCI DSS para mayor información sobre el alcance.

Consulte la *Información Complementaria: Para más información visite la Guía para el Alcance y la Segmentación de PCI DSS*.

Uso de Proveedores de Servicios Externos (TPSP)

Una entidad (el «cliente» en esta sección) puede utilizar un TPSP para almacenar, procesar o transmitir los datos de las cuentas o para administrar los componentes del sistema en su beneficio.

La utilización de TPSP y el cumplimiento del Requisito 12.8 de PCI DSS

Los clientes pueden gestionar y supervisar todas sus relaciones con los TPSP y monitorear el estatus de cumplimiento de PCI DSS de todos los TPSP, de conformidad con el Requisito 12.8, incluidos los TPSP que tienen acceso al CDE del cliente, administran los componentes del sistema dentro del alcance en beneficio del cliente o pueden afectar la seguridad del CDE del cliente.

La gestión de los TPSP, de acuerdo con el Requisito 12.8, incluye realizar una debida diligencia, aplicar los acuerdos adecuados en vigencia, identificar cuáles requisitos se aplican al cliente y cuáles se aplican al TPSP, y monitorear el estado de cumplimiento de los TPSP al menos una vez al año.

El uso de un TPSP compatible con PCI DSS no hace que un cliente cumpla con PCI DSS, ni elimina la responsabilidad del cliente por su propio cumplimiento de PCI DSS.

El Requisito 12.8 no especifica que los TPSP del cliente deben cumplir con PCI DSS, solo que el cliente supervise su estado de cumplimiento. Por lo tanto, los TPSP no requieren cumplir con PCI DSS para que su cliente cumpla con el Requisito 12.8.

Uso de los TPSP para los servicios que cumplen con los requisitos de PCI DSS de los clientes

Cuando el TPSP proporciona un servicio que cumple con los requisitos de PCI DSS en nombre del cliente o cuando ese servicio puede afectar la seguridad del CDE del cliente, esos requisitos están dentro del alcance de la evaluación del cliente y el cumplimiento de ese servicio afectará el cumplimiento de PCI DSS del cliente. El TPSP debe demostrar que cumple con los requisitos de PCI DSS aplicables, para que esos requisitos estén vigentes para sus clientes.

Comprensión de las responsabilidades entre los clientes y los TPSP

Los clientes y los TPSP deberán identificar y entender con precisión los servicios y los componentes del sistema que están incluidos en el alcance de la evaluación de PCI DSS de los TPSP; los requisitos específicos de PCI DSS y los subrequisitos cubiertos por la evaluación de PCI DSS de los TPSP; cualquier requisito que los clientes de los TPSP tengan la obligación de incluir en sus evaluaciones de PCI DSS; y, cualquier otro requisito por el cual haya una responsabilidad compartida por parte de TPSP y de los clientes.

Consulte la *Información Complementaria: Visite las Garantías de Seguridad de Terceros* en el sitio web de PCI SSC para obtener una copia de la plantilla de matriz de responsabilidad que puede utilizarse para documentar y aclarar cómo se comparten las responsabilidades entre los TPSP y los clientes.

Prueba de cumplimiento de PCI DSS y de los TPSP que se proporciona a los clientes

Si un TSPS se somete a su propia evaluación de PCI DSS, se espera que proporcione pruebas suficientes a sus clientes para verificar que el alcance de la evaluación de los TPSP de PCI DSS cubrió los servicios aplicables a los clientes, y que se examinaron y determinaron los requisitos pertinentes de PCI DSS. Si el TPST dispone de una Atestación de Cumplimiento (AOC) se espera que el TPSP la proporcione a los clientes que la soliciten.

Si un TPSP no se somete a su propia evaluación de PCI DSS y, por lo tanto, no cuenta con un AOC, se espera que el TPSP proporcione pruebas específicas relacionadas con los requisitos aplicables de PCI DSS, de modo que los clientes (o sus asesores) puedan confirmar que el TPSP cumple con esos requisitos de PCI DSS.

Implementación de PCI DSS en los Procesos de BAU

Para garantizar que los procesos de control continúen implementándose de manera adecuada, las entidades deben implementar PCI DSS en los procesos de negocio habitual (BAU) como parte de su estrategia de seguridad general. Esto permite que una entidad garantice que los controles de seguridad implementados para asegurar los datos y el entorno continúen implementados de manera adecuada y funcionen correctamente. Algunos requisitos de BAU se definen en el estándar, para ayudar a las entidades a monitorear la efectividad de sus controles de seguridad en forma regular y proporcionar la garantía de que se mantiene el cumplimiento entre las evaluaciones de PCI DSS. Las entidades deben adoptar prácticas de BAU adicionales específicas a sus organizaciones y entorno, siempre que sea posible.

Entre los ejemplos de cómo debe incorporarse PCI DSS a las actividades BAU se incluyen, entre otros, los siguientes:

1. Monitorear los controles de seguridad para asegurarse de que están funcionado de manera eficaz y según lo previsto.
2. Garantizar que todas las fallas en los controles de seguridad se detecten y se respondan con celeridad.
3. Revisar los cambios realizados al entorno (por ejemplo, la adición de nuevos sistemas, los cambios en la configuración del sistema o de la red) antes de completar el cambio, para garantizar que el alcance de PCI DSS esté actualizado y que los controles se aplican como corresponde.
4. Revisar de manera formal el impacto en el alcance y los requisitos de PCI DSS luego de los cambios en la estructura organizacional (por ejemplo, una fusión o adquisición de la compañía).
5. Realizar revisiones y comunicaciones periódicas para confirmar que los requisitos de PCI DSS continúan vigentes y que el personal sigue los procesos establecidos.
6. Revisar las tecnologías de *hardware* y *software* al menos una vez por año para confirmar que continúan siendo respaldadas por el proveedor y que cumplen los requisitos de seguridad de la entidad, incluido PCI DSS, y resolver las fallas cuando corresponda.

Nota: Algunas de las mejores prácticas en esta sección también se incluyen como requisitos de PCI DSS para determinadas entidades. Por ejemplo, aquellos que se someten a una evaluación completa de PCI DSS, los proveedores de servicios que validan los requisitos adicionales de «solo proveedor de servicios» y las entidades designadas que deben validar de acuerdo con el Apéndice A3 de PCI DSS.

Cada entidad debe considerar implementar estas mejores prácticas en su entorno, incluso si no está obligada a validarlas (por ejemplo, los comerciantes que se someten a una autoevaluación).

Comprensión de PCI DSS v4.0

Enfoques para Implementar y Validar PCI DSS

Para proporcionar flexibilidad para las distintas modalidades que las entidades pueden utilizar para cumplir los objetivos de seguridad, PCI DSS v4.0 incluye dos enfoques para implementar los controles y validarlos de acuerdo a PCI DSS. Las entidades deberán identificar el enfoque, o la combinación de enfoques, que mejor se adecue a sus necesidades.

Enfoque Definido – El enfoque tradicional para implementar y validar PCI DSS, es el que las entidades han estado realizando desde el principio para cumplir PCI DSS. Este enfoque utiliza los Requisitos y Procedimientos de Prueba definidos en PCI DSS. La entidad implementa los controles de seguridad que cumplen con los requisitos establecidos, y el asesor sigue los procedimientos de prueba definidos, para verificar que se han cumplido los requisitos. Si una entidad ya tiene los controles implementados que cumplen los requisitos de PCI DSS y está cómoda con su enfoque actual, no hay necesidad de modificarlo. El Enfoque Definido también resulta útil para aquellas que buscan una mayor dirección respecto a cómo cumplir los objetivos de seguridad o para aquellas cuya información de seguridad de PCI DSS resulta nueva.

> **Controles Compensatorios** – Los Controles Compensatorios son todavía una opción válida dentro del Enfoque Definido, para entidades con restricciones técnicas o de negocios legítimas y documentadas, que les impide cumplir el Requisito de Enfoque Definido, tal como está estipulado. La entidad implementará otros controles, o controles compensatorios, para reducir de manera satisfactoria el riesgo asociado al incumplimiento del requisito. Los Controles Compensatorios, en general, se utilizan en situaciones en las que un sistema o proceso tradicional no se puede actualizar para cumplir el requisito.

Enfoque Personalizado – Este enfoque permite a las entidades implementar los controles que cumplan los requisitos establecidos en el *Objetivo de Enfoque Personalizado* de forma tal que no cumplen de manera estricta el requisito definido, dando mayor flexibilidad a las entidades que eligen la implementación de enfoques innovadores o nuevas tecnologías que cumplan los objetivos de PCI DSS. Por ejemplo, algunas entidades pueden optar por complementar sus análisis tradicionales para detectar vulnerabilidades internas con técnicas modernas de aprendizaje automático, tales como User o Entity Behavior Analytics (UEBA), o cualquier otro enfoque de probabilidades de Inteligencia Artificial (AI) para detectar las amenazas avanzadas al CDE. Las soluciones de seguridad modernas emergentes pueden ser candidatas para el Enfoque Personalizado.

CONTROLES COMPENSATORIOS VS. ENFOQUE PERSONALIZADO

Los Controles Compensatorios sirven un propósito distinto de aquel del Enfoque Personalizado. A diferencia de los controles compensatorios, en los que las entidades tienen una restricción que les **impide** cumplir el requisito establecido, con el enfoque personalizado, las organizaciones **eligen cumplir** el requisito de manera distinta a la establecida.

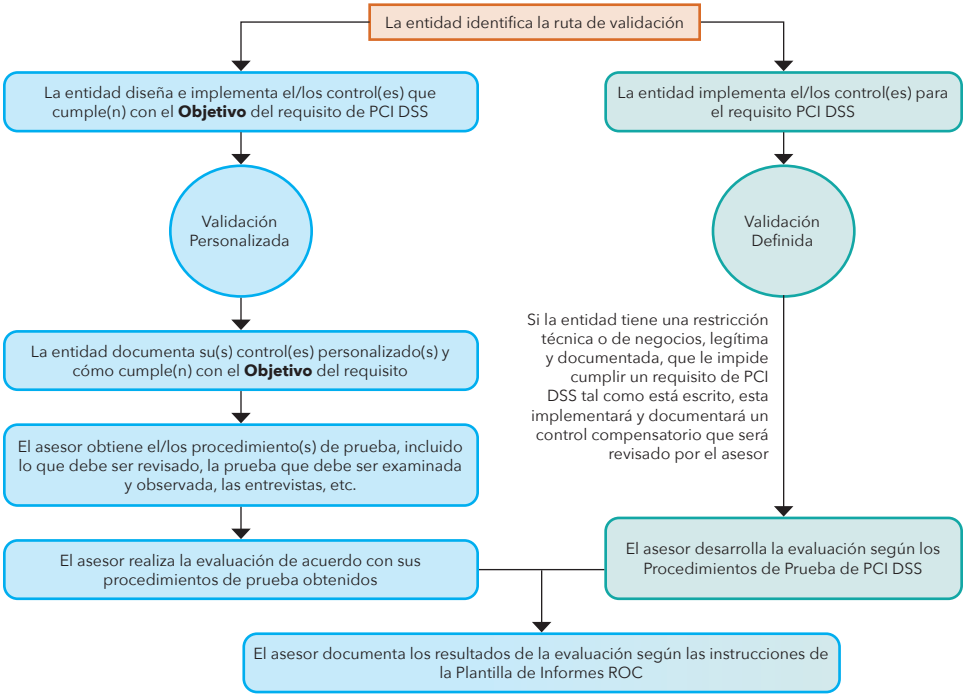
Los controles compensatorios no son una opción con el Enfoque Personalizado.

Debido a que cada implementación personalizada es diferente, no existen procedimientos de prueba definidos. En cambio, el asesor de la entidad desarrolla procedimientos de prueba especiales para verificar que los controles implementados cumplen el *Objetivo del Enfoque Personalizado* establecido.

Con motivo de que las entidades desarrollen su propios controles de seguridad, el Enfoque Personalizado requiere una planificación previa sustancial y documentación anticipada. El Enfoque Personalizado está dirigido a entidades de mayor riesgo que demuestran prácticas de seguridad y de gestión de riesgos robustas y que pueden diseñar, documentar, probar y mantener rigurosos controles de seguridad para cumplir el objetivo.

Las entidades pueden utilizar tanto el enfoque definido como el personalizado dentro de su entorno, el Enfoque Definido para cumplir algunos requisitos y el Enfoque Personalizado para cumplir con otros, o el Enfoque Definido para cumplir un requisito para un componente del sistema o del entorno y el Enfoque Personalizado para cumplir el mismo requisito, pero en otro componente del sistema o del entorno.

Enfoques de Validación de PCI DSS



Comprensión de la Estructura y el Contenido de los Requisitos de PCI DSS

Los títulos de las columnas y el contenido de los requisitos de PCI DSS v4.0 se describen en la página 37 del estándar (ver imagen emergente adyacente y en la URL). Cada requisito incluye los siguientes elementos:

- **La Descripción de los Requisitos** organiza y describe los requisitos correspondientes.
- **El Enfoque Definido** y los **Procedimientos de Prueba del Enfoque Definido** vinculados. Estos procedimientos constituyen el método tradicional de implementación y validación de PCI DSS que utilizan los Requisitos y Procedimientos de Prueba definidos en el estándar.
- **El Objetivo del Enfoque Personalizado** es la meta o el resultado previsto para el requisito. Debe ser cumplido por las entidades que utilicen un Enfoque Personalizado.
- **Las Notas de Aplicabilidad** se aplican tanto al Enfoque Definido como al Personalizado. Estas incluyen información que afecta cómo se interpreta el requisito en el contexto de la entidad o en su alcance. Las Notas de Aplicabilidad también indican los requisitos que son nuevos en PCI DSS v4.0 y cuáles son las prácticas recomendadas hasta el 31 de marzo de 2025.
- **La Guía** proporciona información, categorizada en secciones, para comprender cómo cumplir un requisito. No es necesario seguir la guía, ya que esta no reemplaza ni amplía ningún requisito de PCI DSS.

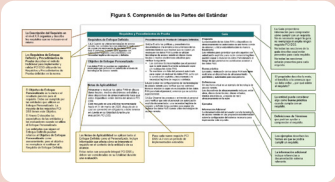


Figura 5. Comprensión de las Partes del Estándar

Seleccione para ver la imagen completa de los detalles anotados en «Comprensión de la información de los Requisitos de PCI DSS»

https://www.pcisecuritystandards.org/understanding-information-in-pci-dss-requirements_/

Resumen de los Requisitos, del 1 al 12, de PCI DSS v4.0

Construir y Mantener Redes y Sistemas Protegidos

En el pasado, el robo de los registro financieros requería que un criminal ingresara físicamente al sitio de negocios de una entidad. Ahora, las transacciones de pago se realizan con distintos dispositivos electrónicos, que incluyen las terminales de pago tradicionales, los dispositivos móviles y otros sistemas informáticos conectados a internet. Al utilizar controles de seguridad de redes, las entidades pueden evitar que los criminales accedan virtualmente a las redes de los sistemas de pagos y roben los datos de las cuentas de pago.

Requisito 1: Instalar y mantener los controles de seguridad de la red

Los controles de seguridad de las redes (NSC), como son los *firewalls* y otras tecnologías de protección de red, constituyen los puntos de aplicación de las políticas de implementación de redes que suelen controlar el tráfico entre dos o más segmentos de red lógicos o físicos (o subredes), basados en políticas o normas predefinidas. Tradicionalmente, esta función ha sido proporcionada por *firewalls* físicos; sin embargo, en la actualidad esta funcionalidad puede ser proporcionada por dispositivos virtuales, controles de acceso en la nube, sistemas de virtualización/contenedores y otras tecnologías de redes definida por *software*.

1.1 Se definen y comprenden los procesos y mecanismos para instalar y mantener los controles de seguridad de la red.

1.2 El acceso a la red desde y hacia el ambiente de datos del titular de la tarjeta está restringido.

1.3 Se restringe el acceso a la red hacia y desde el entorno de los datos de los titulares de la tarjeta.

1.4 Se controlan las conexiones de red entre las redes confiables y las redes no confiables.

1.5 Se mitigan los riesgos para el CDE que pueden provenir de los dispositivos informáticos que pueden llegar a conectarse al CDE o a redes no confiables.

Requisito 2: Aplicar configuraciones seguras a todos los componentes del sistema

Las personas maliciosas, tanto externas como internas de una entidad, a menudo utilizan contraseñas predeterminadas y otras configuraciones predeterminadas del proveedor para comprometer los sistemas. Estas contraseñas y configuraciones son bien conocidas y se determinan fácilmente a través de información pública.

La aplicación de configuraciones seguras a los componentes del sistema disminuye los medios disponibles para que un atacante comprometa el sistema. Cambiar las contraseñas predeterminadas, eliminar *software*, funciones y cuentas innecesarias, y deshabilitar o eliminar servicios innecesarios, ayuda a reducir los potenciales ataques.

2.1 Se definen y comprenden los procesos y mecanismos para aplicar configuraciones seguras a todos los componentes del sistema.

2.2 Los componentes del sistema se configuran y administran de forma segura.

2.3 Los entornos inalámbricos se configuran y gestionan de forma segura.

Proteger los Datos del Tarjetahabiente

Los datos del tarjetahabiente de pago se refieren a cualquier información impresa, procesada, transmitida o almacenada de cualquier manera respecto a una tarjeta de pago. Los datos de cuentas se refieren tanto a los datos del tarjehabientes como a los datos sensibles de autenticación, y se requiere la protección de los datos de las cuentas siempre que los datos de cuentas se almacenen, se procesen o se transmitan. Las entidades que acepten tarjetas de pago deben proteger los datos de las cuentas e impedir su uso no autorizado, ya sea que los datos se impriman o almacenen en el lugar, o se transmitan mediante una red interna o pública a un servidor o proveedor de servicio remoto.

Requisito 3: Proteger los datos de tarjetahabientes almacenados

Los datos de las cuentas de pago no deben almacenarse a menos que esto sea necesario para cumplir las necesidades del negocio. Los datos sensibles de autenticación nunca deben almacenarse después de la autorización. Si su organización almacena PAN, es crucial que se haga ilegible. Si su compañía almacena datos sensibles de autenticación antes de que se complete la autorización, dichos datos también deben ser protegidos[1].

3.1 Se definen y comprenden los procesos y mecanismos para proteger los datos de las cuentas almacenados.

3.2 El almacenamiento de los datos de cuentas se reduce al mínimo.

3.3 Los datos sensibles de autenticación (SAD) no se almacenan después de su autorización.

3.4 El acceso a la visualización del PAN completo y la capacidad de copiar los datos de titulares de tarjetas están restringidos.

3.5 El número de cuenta principal (PAN) está protegido dondequiera que se almacene.

3.6 Las claves criptográficas utilizadas para proteger los datos almacenados del tarjetahabiente están protegidos.

3.7 Cuando se utiliza la criptografía para proteger los datos almacenados del tarjetahabiente se definen e implementan procesos y procedimientos de gestión de claves que cubren todos los aspectos del ciclo de vida de las mismas.

1 Este requisito es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.

INTRODUCCIÓN AL CIFRADO

La Criptografía utiliza una fórmula matemática que convierte un texto simple en ilegible para personas que no cuentan con un conocimiento especial (una «llave»). La Criptografía se aplica a los datos almacenados, así como a los datos que se transmiten a través de una red.

El cifrado convierte el texto simple en un texto codificado.

El Descifrado convierte el texto codificado en un texto simple.

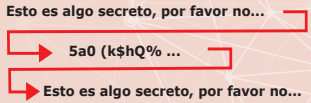


Ilustración: Wikimedia Commons

Elementos de los Datos de las Cuentas y Requisitos de Almacenamiento

La Tabla 3 de PCI DSS (ver más abajo) identifica los elementos relacionados con los datos del tarjehabientes y los datos sensibles de autenticación, ya sea que se permita o se prohíba el almacenamiento de cada elemento de los datos, o que cada elemento de los datos deba hacerse ilegible –por ejemplo, con un cifrado complejo– cuando se almacena. Esta tabla no es exhaustiva y se presenta solo para ilustrar cómo se aplican los requisitos establecidos a los diferentes elementos de los datos.

		Elementos de los Datos	Restricciones de Almacenamiento	Condiciones Requeridas para que los Datos Almacenados sean Ilegibles
Datos de las Cuentas	Datos del Titular de la Tarjeta	Número de Cuenta Principal (PAN)	El Almacenamiento se reduce al mínimo, tal como se define en el Requisito 3.2	Sí, como se define en el Requisito 3.5
		Nombre del titular de la tarjeta	El Almacenamiento se reduce al mínimo, tal como se define en el Requisito 3.2[2]	No
		Código de Servicio		
		Fecha de Expiración		
	Datos Confidenciales de Autenticación	Datos de Pista Completo	No pueden almacenarse después de la autorización, tal como se define en el Requisito 3.3.1[3]	Sí, los datos almacenados hasta que se complete la autorización deben estar protegidos con criptografía sólida compleja como se define en el Requisito 3.3.2
		Código de Verificación de la Tarjeta		
		PIN y Bloque de PIN		

2 Cuando los datos existen en el mismo entorno que los datos PAN.

3 Salvo lo permitido para los emisores y las empresas que apoyan los servicios de emisión. Los requisitos para emisores y servicios de emisión se definen por separado en el Requisito 3.3.3.

Requisito 4: Proteger los datos de tarjetahabientes con criptografía robusta durante la transmisión a través de redes abiertas y publicas

Para evitar que sean vulnerados, los Números de Cuenta Principal (PAN) deben estar cifrados durante la transmisión a través de redes a las que las personas maliciosas puedan acceder fácilmente, incluidas las redes públicas y no confiables. Las redes inalámbricas mal configuradas y las vulnerabilidades de los cifrados tradicionales y los protocolos de autenticación continúan siendo el objetivo de personas maliciosas que buscan aprovechar estas vulnerabilidades para obtener un acceso privilegiado a los entornos de los datos del tarjehabientes (CDE). Las transmisiones de los PAN pueden ser protegidas, cifrando los datos antes de que estos sean transmitidos o cifrando la sesión a través de la cual se transmiten los datos, o ambos.

4.1 Los procesos y mecanismos para proteger los datos de los titulares de tarjetas con criptografía sólida durante la transmisión a través de redes públicas abiertas están definidos y documentados.

4.2 Los PAN están protegidos con criptografía sólida durante la transmisión.

Mantener un Programa de Gestión de Vulnerabilidades

La gestión de vulnerabilidades comprende el proceso de encontrar y mitigar, de manera sistemática y continua, las debilidades del entorno de una entidad de tarjetas de pago. Esto incluye la resolución de amenazas de *software* malicioso, identificar y emparchar de forma periódica las vulnerabilidades y asegurar que el *software* se desarrolle de manera segura y sin vulnerabilidades de código conocidas.

Requisito 5: Proteger todos los sistemas y redes de software malicioso

El software malicioso (malware) es un *software* o *firmware* diseñado para infiltrarse o dañar un sistema informático sin el conocimiento o el consentimiento del propietario, con la intención de comprometer la confidencialidad, la integridad o la disponibilidad de los datos del propietario, las aplicaciones o el sistema operativo. Algunos ejemplos incluyen a los virus, gusanos, troyanos, *software* espía (spyware), *software* secuestrador (ransomware), *keyloggers* y *rootkits*, el código malicioso, las secuencias de comandos y los enlaces. Los *softwares* maliciosos pueden entrar en la red durante muchas actividades aprobadas para el negocio, incluido el correo electrónico de los empleados (por ejemplo, a través del *phishing*) y el uso de Internet, los ordenadores móviles y los dispositivos de almacenamiento, lo que resulta en un aprovechamiento de las vulnerabilidades del sistema.

GESTIÓN DE VULNERABILIDADES

Crear una política que regule los controles de seguridad de acuerdo a los estándares de la industria y las buenas prácticas.

Analizar los sistemas periódicamente en busca de vulnerabilidades.

Crear un calendario de soluciones basado en el riesgo y la prioridad.

Realizar pruebas previas e **implementar** parches.

Volver a analizar para verificar que las vulnerabilidades han sido resueltas.

Actualizar todo el *software* con las más recientes características y tecnologías.

Utilizar solo software o sistemas que sean desarrollados de manera segura en consonancia con los estándares de buenas prácticas de la industria.

5.1 Se definen y comprenden los procesos y mecanismos para proteger todos los sistemas y redes del software malintencionado.

5.2 El software malintencionado (malware) es evadido, o se detecta y se soluciona.

5.3 Los mecanismos y procesos antivirus están activos, mantenidos y monitoreados.

5.4 Los mecanismos contra el phishing protegen a los usuarios contra los ataques de fraude informático.

Requisito 6: Desarrollar y mantener sistemas y softwares seguros

Las vulnerabilidades de seguridad de los sistemas y de las aplicaciones pueden permitir a los criminales tener acceso a los datos de pago. Muchas de estas vulnerabilidades se eliminan con la instalación de parches de seguridad proporcionados por el proveedor, que realizan un trabajo de reparación rápida para una parte específica del código de programación. Todos los componentes del sistema deben contar con la instalación de los más recientes parches de seguridad para prevenir el aprovechamiento. Las entidades también deberán aplicar los parches a los sistemas menos críticos en un marco de tiempo correspondiente, en base a un análisis de riesgo formal. Las aplicaciones deben desarrollarse de acuerdo a un desarrollo seguro y a las prácticas de codificación, y los cambios a los sistemas en el entorno de los datos del tarjehabientes deben cumplir con los procedimientos de control de cambios.

6.1 Se definen y comprenden los procesos y mecanismos para desarrollar y mantener sistemas y software seguros.

6.2 El software a medida y personalizado se desarrolla de forma segura.

6.3 Las vulnerabilidades de seguridad se identifican y son abordadas.

6.4 Las aplicaciones web públicas están protegidas contra ataques.

6.5 Los cambios en todos los componentes del sistema se gestionan de forma segura.

Por lo general, el *software* por encargo se desarrolla por un tercero en beneficio de la entidad, mientras que el *software* personalizado se desarrolla por la entidad de manera interna.

Implementar Medidas Sólidas de Control de Acceso

El acceso a los datos de las cuentas de pago será concedido solo en función de lo que el negocio necesita saber. Los controles de acceso lógicos son medios técnicos que se utilizan para permitir o denegar el acceso a los datos en los sistemas informáticos. Los controles de acceso físico comprenden el uso de bloqueos o de otros medios físicos para restringir el acceso al soporte informático, a los registros en papel físico y a los sistemas informáticos.

Requisito 7: Restringir el acceso a los componentes del sistema y a los datos de tarjetahabientes según la necesidad de conocimiento de la empresa

Las personas no autorizadas pueden obtener acceso a los datos o a los sistemas críticos debido a reglas y definiciones de control de acceso ineficientes. Para garantizar que solo el personal autorizado pueda tener acceso a los datos críticos, se deben implementar sistemas y procesos para limitar el acceso según la necesidad de saber y de acuerdo con las responsabilidades de cada puesto de trabajo. La «necesidad de saber» se refiere a proporcionar acceso solo a la cantidad de datos necesaria para realizar un trabajo. Los «privilegios mínimos» se refieren a proporcionar únicamente el nivel mínimo de privilegios necesarios para realizar un trabajo.

7.1 Se definen y comprenden los procesos y mecanismos para restringir el acceso a los componentes del sistema y a los datos del tarjehabientes según la necesidad de saber del negocio.

7.2 El acceso a los componentes y datos del sistema se define y asigna adecuadamente.

7.3 El acceso a los componentes y datos del sistema se gestiona a través de un sistema de control de acceso.

¡LA RESTRICCIÓN DEL ACCESO ES CRUCIAL!

Restringir el acceso a los entornos de los datos de los titulares de las tarjetas a través de la utilización de controles de acceso físicos y lógicos.

Limitar el acceso solo a aquellos individuos cuyo trabajo requiere dicho acceso.

Formalizar una política de control de acceso que incluya una lista de quiénes tienen acceso a los datos de las cuentas específicos y a los sistemas.

Negar todo acceso a quien no esté específicamente autorizado para acceder a los datos de los titulares de las tarjetas y a los sistemas.

Foto: Wikimedia Commons

Requisito 8: Identificar a los usuarios y autenticar el acceso a los componentes del sistema

Asignar una identificación única (ID) a cada persona con acceso garantiza que las acciones que se tomen en relación a los datos críticos o a los sistemas, pertenezcan o puedan rastrearse a los usuarios conocidos y autorizados. A menos que se disponga lo contrario en el requisito, estos requisitos son aplicables a todas las cuentas, incluidas las cuentas de puntos de venta, aquellas con capacidades administrativas y todas las cuentas que se utilicen para ver o acceder a los datos de las cuentas o a los sistemas con dichos datos. Estos requisitos no se aplican a las cuentas utilizadas por los consumidores (titulares de las tarjetas).

8.1 Los procesos y mecanismos para identificar a los usuarios y autenticar el acceso a los componentes del sistema están definidos y son comprendidos.

8.2 La identificación de usuarios y las cuentas relacionadas para usuarios y administradores se gestionan estrictamente durante el ciclo de vida de una cuenta.

8.3 Se establece y gestiona una autenticación robusta para usuarios y administradores.

8.4 Se implementa la autenticación de múltiples factores (MFA) para proteger el acceso al CDE.

8.5 Los sistemas de autenticación de múltiples factores (MFA) están configurados para evitar su uso indebido.

8.6 El uso de cuentas de aplicaciones y sistemas y los factores de autenticación asociados se gestionan estrictamente.

DEFINIR Y AUTENTICAR A TODOS LOS USUARIOS

Cada usuario que cuente con acceso al entorno de los datos de los titulares de las tarjetas debe tener un único ID. Esto permite que el negocio pueda rastrear cada actividad a una persona específica. Cada usuario deberá contar con un mecanismo robusto de autenticación —como una contraseña sólida, un sistema biométrico o el acceso a través de un token— y utilizar una autenticación de factores múltiples para todos los accesos al CDE [4].

Foto: Wikimedia Commons

4 Este requisito para el uso de autenticación de factores múltiples de todo acceso al CDE es una práctica recomendada hasta el 31 de marzo de 2025, después de lo cual deberá tenerse en cuenta en su totalidad durante una evaluación PCI DSS.

Requisito 9: Restringir el acceso físico a los datos de tarjetahabientes

El acceso físico a los datos del tarjehabientes o a los sistemas que almacenan, procesan o transmiten los datos del tarjehabientes, deberá estar restringido, de manera que las personas no autorizadas no puedan acceder o eliminar los sistemas o realizar copias impresas que contengan dichos datos.

9.1 Los procesos y mecanismos para restringir el acceso físico a los datos de titulares de tarjetas están definidos y comprendidos.

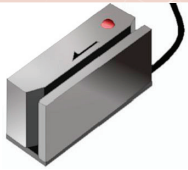
9.2 Los controles de acceso físico gestionan la entrada a las instalaciones y sistemas que contienen datos de titulares de tarjetas.

9.3 El acceso físico del personal y de los visitantes está autorizado y gestionado.

9.4 Los medios con datos de titulares de tarjetas se almacenan, acceden, distribuyen y destruyen de forma segura.

9.5 Los dispositivos de punto de interacción (POI) están protegidos contra manipulaciones y sustituciones no autorizadas.

LOS COMERCIANTES DEBEN INSPECCIONAR LOS DISPOSITIVOS DE PAGO



Los delincuentes intentan robar los datos de tarjetas de pago robando y/o manipulando los dispositivos y las terminales de lectura de las tarjetas. Los comerciantes deben inspeccionar los dispositivos de pago de forma periódica en busca de componentes de *skimming* o de otras maneras de manipulación (véase el Requisito 9.5.1 de PCI DSS).

- Mantener una lista de dispositivos de punto de interacción (POI).
- Inspeccionar de forma periódica los dispositivos POI en busca de falsificaciones o de otros reemplazos no autorizados.
- Capacitar al personal para que esté alerta a los comportamientos sospechosos y para que informe la manipulación o las sustituciones de los dispositivos no autorizadas.

Ilustración: Wikimedia Commons

Monitorear y Verificar las Redes Regularmente

Las conexiones físicas, virtuales e inalámbricas son el adhesivo que conecta todos los puertos y servidores en la infraestructura de pagos. Las vulnerabilidades en los dispositivos de conexión o en los sistemas presentan oportunidades a los criminales para obtener acceso no autorizado a las aplicaciones de pago y a los datos de las cuentas de pago. Para evitar el aprovechamiento, las entidades deben monitorear y evaluar las redes de manera periódica, para descubrir y resolver accesos y actividades inesperadas, fallas en el sistema de seguridad y vulnerabilidades.

Requisito 10: Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabientes

Los mecanismos de ingreso y la posibilidad de rastrear las actividades de los usuarios son claves para detectar anomalías o actividades sospechosas y para realizar análisis forenses eficaces. La presencia de registros en todos los entornos permite el seguimiento, las alertas y los análisis exhaustivos cuando algo sale mal. Determinar la causa de una situación comprometida es difícil, si no imposible, sin los registros de actividad del sistema.

10.1 Se definen y documentan los procesos y mecanismos para ingresar y monitorear todos los accesos a los componentes del sistema y a los datos de titulares de tarjetas.

10.2 Los registros de auditoría se implementan para respaldar la detección de anomalías y actividades sospechosas, y el análisis forense de eventos.

10.3 Los registros de auditoría están protegidos contra la destrucción y las modificaciones no autorizadas.

10.4 Los registros de auditoría se revisan para identificar anomalías o actividades sospechosas.

10.5 El historial del registro de auditoría se conserva y está disponible para su análisis.

10.6 Los mecanismos de sincronización de la hora admiten una configuración de hora coherente en todos los sistemas.

10.7 Las fallas de los sistemas críticos de control de seguridad se detectan, se reportan y se responden de manera oportuna.

MONITOREO DE TODAS LAS ACTIVIDADES

10.2.2 Los registros de auditoría guardan los siguientes detalles para cada evento auditable:

- Identificación del usuario
- Tipo de evento
- Fecha y hora
- Indicación de Exitoso o Fallido
- Origen del evento
- La identificación o el nombre de los datos, los componentes del sistema, los recursos o servicios afectados (por ejemplo, el nombre y el protocolo).

Foto: Wikimedia Commons

Requisito 11: Poner a prueba regularmente la seguridad de los sistemas y de las redes

Se descubren vulnerabilidades continuamente por parte de expertos y personas malintencionadas y también se crean a través de nuevos *softwares*. Los componentes del sistema, los procesos y el *software* por encargo y el personalizado deben probarse con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno cambiante.

11.1 Se definen y comprenden los procesos y mecanismos para probar periódicamente la seguridad de los sistemas y redes.

11.2 Los puntos de acceso inalámbrico se identifican y monitorean, y se abordan los puntos de acceso inalámbrico no autorizados.

11.3 Las vulnerabilidades internas y externas se identifican regularmente, son priorizadas y atendidas

11.4 Las pruebas de penetración externas e internas se realizan regularmente y las vulnerabilidades explotables y las debilidades en materia de seguridad son corregidas.

11.5 Las intrusiones en la red y los cambios de archivos inesperados se detectan y responden

11.6 Los cambios no autorizados en las páginas de pago se detectan y responden

CONSEJOS PARA REALIZAR LOS ANÁLISIS

Reciba Asesoramiento. Pregunte a su banco adquirente sobre cualquier vínculo que este tenga con los Proveedores de Análisis Aprobado (ASV) de PCI.

Converse con un ASV de PCI. Visite el sitio web de PCI Council para acceder a la lista de ASV de PCI.

Seleccione un ASV. Contacte a varios ASV de PCI y seleccione el programa más conveniente.

Atienda las Vulnerabilidades. Solicite ayuda a su ASV de PCI para resolver los problemas identificados con el análisis.

ANÁLISIS DE VULNERABILIDADES EN LOS NIVELES DE GRAVEDAD

Puntaje de CVSS	Nivel de Seguridad	Resultados del Análisis
Del 7.0 al 10.0	Gravedad Alta	Desaprobado
Del 4.0 al 6.9	Gravedad Media	Desaprobado
Del 0.0 al 3.9	Gravedad Baja	Aprobado

El análisis de vulnerabilidades externas debe realizarse al menos una vez cada tres meses por un Proveedor de Análisis Aprobado por PCI SSC (ASV). Para recibir un «aprobado» el informe externo del análisis no debe incluir ninguna vulnerabilidad a la que se le otorgue un puntaje del Sistema de Análisis de Vulnerabilidades Comunes (CVSS) que sea igual o mayor que 4.0, o cualquier vulnerabilidad con características o configuraciones que infrinjan PCI DSS.

Mantener una Política de Protección Informática

Una política de seguridad sólida establece las pautas de seguridad que afectan a toda compañía de la entidad, e informa a los empleados de sus obligaciones respecto a la seguridad. Todo el personal debe ser consciente de la confidencialidad de los datos de las tarjetas y de sus responsabilidades para protegerlos.

Requisito 12: Respaldar la seguridad de la información con políticas y programas organizacionales

12.1 Una política integral de seguridad de la información, que rija y proporcione orientación para la protección de los activos de información de la entidad, es actualizada y bien conocida.

12.2 Se definen e implementan políticas de uso aceptable para las tecnologías orientadas al usuario final.

12.3 Los riesgos para el entorno de datos de titulares de tarjetas se identifican, evalúan y gestionan formalmente.

12.4 Gestión del cumplimiento con PCI DSS.

12.5 Documentación y validación del alcance PCI DSS.

12.6 La educación en concienciación sobre la seguridad es una actividad continua.

12.7 El personal es evaluado para reducir los riesgos de las amenazas internas.

12.8 Gestión del riesgo para los activos de información asociados a las relaciones con proveedores de servicios de terceros (TPSP).

12.9 Los proveedores de servicios de terceros (TPSP) respaldan el cumplimiento de sus clientes con PCI DSS.

12.10 Respuesta inmediata a incidentes de seguridad sospechosos y confirmados que podrían afectar al CDE.

Recursos

Sitio web PCI Security Standards Council

Preguntas Frecuentes (FAQs)

Blog del PCI SSC

Suscríbase al PCI Perspectives Blog

Información de Membresías

Recursos para los Comerciantes

Entrenamiento

Productos y Soluciones Calificadas de PCI

Profesionales Calificados de PCI

Estándar de Seguridad de Datos (PCI DSS)

Glosario

Centro de Amenazas

Acerca de PCI Security Standards Council

PCI Security Standards Council (PCI SSC) es un foro global a través del cual la industria se reúne y desarrolla, refuerza, difunde y asiste la comprensión de los estándares de seguridad para la protección de las cuentas de pago.

PCI SSC mantiene, desarrolla y promueve los Estándares de Seguridad de Payment Card Industry. También proporciona las herramientas críticas que se necesitan para la implementación de los estándares, tales como las calificaciones de evaluación y análisis, los cuestionarios de autoevaluación, el entrenamiento y educación y los programas de certificación de productos.

PCI SSC está liderado por un Comité Ejecutivo que establece las políticas, compuesto por los representantes de los Miembros Fundadores y de los Miembros Estratégicos. American Express, Discover Financial Services, JCB International, Mastercard, UnionPay y Visa Inc.

La membresía como Organización Participante de PCI SSC está abierta de manera global para aquellos que estén vinculados a la industria de pagos, incluidos los comerciantes, los bancos, los procesadores, los desarrolladores de *hardware* y *software* y los proveedores de los puntos de venta.

Se recomienda a las partes interesadas de la industria que se unan a PCI SSC como miembros Estratégicos o Afiliados y Organizaciones Participantes para revisar las adiciones propuestas o las modificaciones hechas a los estándares.

MARCAS DE PAGO PARTICIPANTES DE PCI SSC

ORGANIZACIONES PARTICIPANTES

Los Comerciantes, los Proveedores de Servicios, los Nancos, los Procesadores, los Desarrolladores y los Proveedores en los Puntos de Venta.

Estándar de Seguridad de Datos PCI

PCI DSS proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos de las cuentas de pago. Conozca más sobre los requisitos, los controles y procesos de seguridad y los pasos para evaluar el cumplimiento en la Guía de Referencia Rápida de PCI DSS.

Objetivos	Requisitos de PCI DSS
Construir y Mantener Redes y Sistemas Protegidos	1. Instalar y mantener los controles de seguridad de la red 2. Aplicar configuraciones seguras a todos los componentes del sistema
Proteger los Datos del Tarjetahabiente	3. Proteger los datos de tarjetahabientes almacenados 4. Proteger los datos de tarjetahabientes con criptografía robusta durante la transmisión a través de redes abiertas y publicas
Mantener un Programa de Gestión de Vulnerabilidades	5. Proteger todos los sistemas y redes de software malicioso 6. Desarrollar y mantener sistemas y softwares seguros
Implementar Medidas Sólidas de Control de Acceso	7. Restringir el acceso a los componentes del sistema y a los datos de tarjetahabientes según la necesidad de conocimiento de la empresa 8. Identificar a los usuarios y autenticar el acceso a los componentes del sistema 9. Restringir el acceso físico a los datos de tarjetahabientes
Monitorear y Verificar las Redes Regularmente	10. Registrar y supervisar todos los accesos a los componentes del sistema y a los datos de tarjetahabientes 11. Poner a prueba regularmente la seguridad de los sistemas y de las redes
Mantener una Política de Protección Informática	12. Respaldar la seguridad de la información con políticas y programas organizacionales