

RECURSOS DE PROTECCIÓN DE PAGOS PARA PEQUEÑOS COMERCIANTES

Guía de pagos seguros

Versión 1.0 | julio de 2016



COMPRENDA CUÁL ES SU RIESGO	4
PROTEJA SU EMPRESA CON ESTOS ELEMENTOS DE SEGURIDAD BÁSICOS	6
DÓNDE OBTENER AYUDA	20



**COMPRENDA CUÁL
ES SU RIESGO**

Comprenda cuál es su riesgo

Como pequeña empresa, usted es uno de los blancos principales de los ladrones de datos.

Cuando se filtran los datos de la tarjeta de pago, los daños colaterales golpean rápidamente. Sus clientes pierden la confianza en su capacidad de proteger su información personal. Se van a hacer negocios a otra parte. Podrían surgir multas y daños financieros a consecuencia de demandas legales, y su empresa puede perder la capacidad de aceptar tarjetas de pago. Una encuesta realizada a 1015 pequeñas y medianas empresas indicó que el 60 % de esas empresas que sufrieron la filtración de datos cierran en

seis meses. Encuesta de la Alianza Nacional para la Seguridad Cibernética (National Cyber Security Alliance survey, NCSA)

El
60 %



DE PEQUEÑAS EMPRESAS EXPERIMENTARON UNA FILTRACIÓN DE DATOS CIBERNÉTICA (Gobierno del Reino Unido)



El
71 %

DE LOS HACKERS ATACAN A EMPRESAS CON MENOS DE 100 EMPLEADOS (Verizon 2012)

\$20 752



COSTO PROMEDIO PARA UNA PEQUEÑA EMPRESA DEBIDO AL ACCESO ILEGAL, QUE AUMENTÓ DE \$8600 EN 2013

Asociación Nacional de Pequeñas Empresas (National Small Business Association, NSBA)

El
69 %



DE LOS CONSUMIDORES ESTADOUNIDENSES SE PREOCUPAN POR EL ROBO DE LOS DATOS DE SUS TARJETAS DE PAGO (Gallup)

¿Qué es lo que está en riesgo?

LOS DATOS DE LAS TARJETAS DE SUS CLIENTES SON UNA MINA DE ORO PARA LOS DELINCUENTES. ¡NO PERMITA QUE ESTO LE SUCEDA!

Siga las medidas de esta guía para proteger sus tarjetas del robo de datos.

Los ejemplos de los datos de las tarjetas de pago corresponden al número de cuenta principal (PAN) y a un código de seguridad de tres o cuatro dígitos. Las flechas rojas debajo señalan los tipos de datos que requieren protección.

TIPOS DE DATOS EN UNA TARJETA DE PAGO



¿QUÉ ES LA PCI DSS?

La Norma de seguridad de datos de la Industria de tarjetas de pago (PCI DSS) es un conjunto de requisitos de seguridad que puede ayudar a los pequeños comerciantes a proteger los datos de la tarjeta del cliente que se encuentran en las tarjetas de pago.

Es posible que los pequeños comerciantes estén familiarizados con la validación del cumplimiento de la PCI DSS a través de un Cuestionario de autoevaluación (SAQ).

Para obtener más información sobre la PCI DSS, consulte los Recursos al final de esta guía.

Comprenda su sistema de pago: términos de pago comunes

Según el lugar del mundo en el que se encuentre, el equipo que se utiliza para registrar los pagos tiene diferentes nombres. Aquí le mostramos los tipos que mencionamos en este documento y cómo se llaman comúnmente.



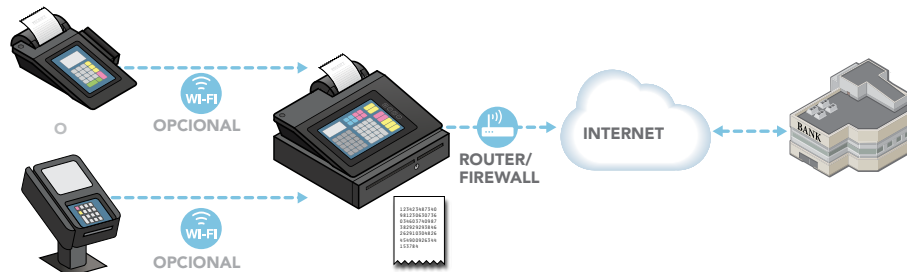
Un **TERMINAL DE PAGO** es el dispositivo que se utiliza para registrar los pagos con tarjeta del cliente ya sea al pasar, deslizar, insertar, teclear o ingresar manualmente el número de la tarjeta. Terminal de puntos de venta o (POS), máquina de tarjeta de crédito, terminal de proceso rápido de datos (Process Data Quickly, PDQ) o terminal EMV (Europay, MasterCard y Visa)/habilitados para chip también son nombres que se utilizan para describir estos dispositivos.



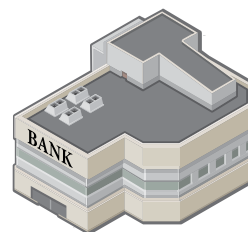
Una **CAJA REGISTRADORA ELECTRÓNICA** registra y calcula transacciones y puede imprimir recibos, pero no acepta pagos con tarjeta del cliente.



Un **TERMINAL DE PAGO INTEGRADO** es un terminal de pago y una caja registradora electrónica en un solo dispositivo, lo que significa que acepta pagos con tarjeta, registra y calcula las transacciones e imprime recibos.



Un **SISTEMA DE PAGO** abarca el proceso completo de la aceptación de pagos con tarjeta en una tienda minorista (incluye tiendas/comercios y escaparates de comercio electrónico). Este puede incluir un terminal de pago, una caja registradora electrónica, otros dispositivos o sistemas conectados a un terminal de pago (por ejemplo, Wi-Fi para conectividad o una computadora que se utilice para inventario), servidores con componentes de comercio electrónico como páginas de pagos, y las conexiones con un banco comercial.



Un **BANCO COMERCIAL** es un banco o una institución financiera que procesa pagos con tarjeta de débito/crédito en nombre de los comerciantes. El adquirente, el banco adquirente y procesador de pago o tarjeta son términos que también se utilizan para esta entidad.

¿De qué forma está en riesgo su empresa?

Cuanto más funciones tenga su sistema de pago, más difícil es protegerlo. Generalmente, estas funciones adicionales les facilitan el camino a los delincuentes para robar los datos de la tarjeta de su cliente. Piense detenidamente si realmente necesita estas funciones adicionales (por ejemplo, Wi-Fi o cámaras) para su empresa.

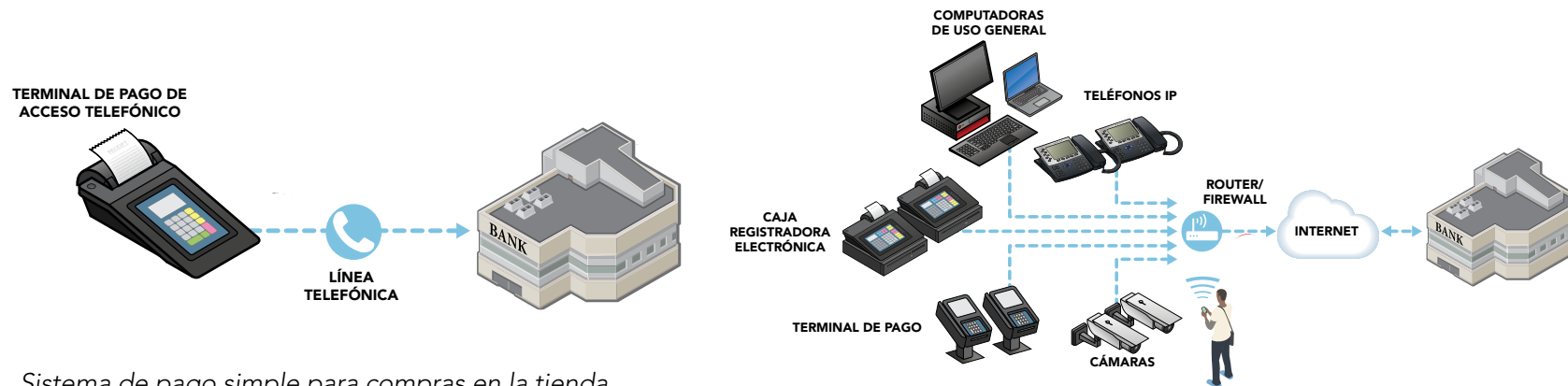


¿Cómo vende sus productos o servicios? Existen tres maneras principales:

1. Una persona ingresa a su tienda y hace una compra con su tarjeta.
2. Una persona visita su sitio web y paga en línea.
3. Una persona llama a su tienda y ofrece detalles de la tarjeta por teléfono, o envía los detalles por correo o fax.

Comprenda cuál es su riesgo: tipos de sistemas de pago

Sus riesgos de seguridad varían ampliamente según la complejidad de su sistema de pago, ya sea de manera personal o en línea.



Sistema de pago simple para compras en la tienda

Sistema de pago complejo para compras en la tienda, con Wi-Fi, cámaras, teléfonos con acceso a Internet y otros sistemas conectados



Sistema de pago de comercio electrónico complejo para compras de la tienda en línea; el comerciante administra su propio sitio web y página de pagos











































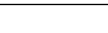





Utilice los Sistemas de pagos comunes que lo ayudarán a identificar qué tipo de sistema de pago utiliza, su riesgo y los consejos de seguridad recomendados como un punto de partida para que dialogue al respecto con su banco comercial y socios proveedores.



**PROTEJA SU
EMPRESA CON ESTOS
ELEMENTOS DE
SEGURIDAD BÁSICOS**

¿Cómo protege su empresa?

La buena noticia es que puede empezar a proteger su empresa hoy con estos elementos básicos de seguridad:

Cómo proteger su empresa contra las filtraciones de datos	Costo	Nivel de complejidad	Mitigación de riesgos
 Utilice contraseñas seguras y cambie las predeterminadas			
 Proteja los datos de su tarjeta y solo guarde lo que necesita			
 Revise los terminales de pago para detectar alguna alteración			
 Instale parches provistos por sus proveedores			
 Utilice socios comerciales de confianza y sepa cómo contactarlos			
 Proteja el acceso del personal interno a los datos de su tarjeta			
 No les facilite a los hackers el acceso a su sistema			
 Utilice un software antivirus			
 Realice un análisis de vulnerabilidades y arregle los problemas			
 Utilice soluciones y terminales de pago seguros			
 Proteja su empresa de Internet			
 Para tener la mejor protección, convierta los datos de su tarjeta en información inutilizable para los delincuentes			

Estos elementos básicos de seguridad están organizados desde el método más simple y el costo de implementación más bajo hasta el sistema más complejo y el costo de implementación más alto. Además, el índice de reducción de riesgos que cada uno ofrece a los pequeños comerciantes se indica en la columna "Mitigación de riesgos".



Utilice contraseñas seguras y cambie las predeterminadas

Costo



Nivel de complejidad



Mitigación de riesgos



Sus contraseñas son fundamentales para la seguridad de la computadora y de los datos de la tarjeta. Así como una cerradura en su puerta protege la propiedad física, una contraseña ayuda a proteger sus datos comerciales. Además, tenga en cuenta que el equipo de computadoras y el software listo para instalar (incluido su terminal de pago) generalmente vienen con contraseñas predeterminadas como "contraseña" o "admin", que son comúnmente conocidas por los hackers y son fuentes frecuentes de filtraciones de los pequeños comerciantes.

Aproximadamente

un
80 %

de las filtraciones de datos tienen que ver con contraseñas robadas o adivinadas

Verizon PCI 2015

CAMBIE SUS CONTRASEÑAS CON REGULARIDAD.

Trate a sus contraseñas como a un cepillo de dientes. No deje que nadie las utilice y cámbielas por unas nuevas cada tres meses.

BUSQUE AYUDA. Pregúntele a sus proveedores o proveedores de servicios sobre las contraseñas predeterminadas y cómo cambiarlas. Luego, ¡hágalo!

ELIJA CONTRASEÑAS DIFÍCILES DE ADIVINAR.

Las contraseñas más comunes son "contraseña" y "123456." Los hackers intentan con las contraseñas que son fáciles de adivinar porque la mitad de las personas las utilizan. Una contraseña segura tiene siete o más caracteres y una combinación de letras mayúsculas y minúsculas, números y símbolos (como !@#\$&*). Una frase también puede ser una contraseña segura (y puede ser fácil de recordar), como "PaP4sB1g&Mac".

NO LA COMPARTA. Exija que cada empleado tenga su propia contraseña e identificación de inicio de sesión y ¡que nunca las compartan!

Para obtener más información sobre la seguridad de contraseñas, consulte estos recursos en el sitio web del Consejo de la PCI:

INFOGRAFÍA

Es momento de cambiar su contraseña



VIDEO

Aprenda sobre la seguridad de las contraseñas en 2 minutos



Contraseñas predeterminadas comunes que se DEBEN cambiar:

[ninguna]

[nombre del producto/proveedor]

1234 o 4321

acceso

admin

anónimo

basededatos

huésped

gerente

contr

contraseña

raíz

sa

secreto

admdelsist

usuario



Proteja los datos de su tarjeta y solo guarde lo que necesita

Costo



Nivel de complejidad



Mitigación de riesgos



Es imposible proteger los datos de la tarjeta si no sabe dónde están.

¿Qué puede hacer?

La tokenización tiene un objetivo similar al cifrado, pero funciona de manera distinta. Sustituye los datos de la tarjeta con datos sin importancia (un "token") que no tiene valor para un hacker.

PREGÚNTELE A UN EXPERTO. Pregúntele a su banco comercial o proveedor de terminal de pago dónde sus sistemas almacenan los datos y si usted puede simplificar la forma de procesar los pagos. Además, pregunte cómo realizar transacciones específicas (por ejemplo, para pagos recurrentes) sin guardar el código de seguridad de la tarjeta.

TERCERICE. La mejor forma de protegerse contra las filtraciones de datos es evitar absolutamente almacenar datos de tarjeta. Considere la posibilidad de tercerizar su procesamiento de tarjetas con un proveedor de servicios que cumpla con la PCI DSS. Consulte los Recursos en la página 22 para obtener la lista de proveedores de servicios que cumplen con la PCI DSS.

SI NO NECESITA LOS DATOS DE LA TARJETA, NO LOS GUARDE. Destruya o triture de forma segura los datos de la tarjeta que no necesita. Si necesita conservar un papel con datos confidenciales de la tarjeta, tache los datos con un marcador negro grueso hasta que no se puedan leer y guarde el papel en un cajón con cerradura o una caja fuerte a los que solo accedan pocas personas.

LIMITE EL RIESGO. En lugar de aceptar detalles del pago por correo electrónico, solicíteles a sus clientes que los envíen por teléfono, fax o correo tradicional.

USE TOKENIZACIÓN O CIFRADO. Pregúntele a su banco comercial si usted REALMENTE necesita guardar los datos de la tarjeta. Si lo hace, pregúntele a su banco comercial o proveedor de servicios sobre las tecnologías de cifrado o tokenización que convierten los datos de la tarjeta en información inutilizable incluso si los roban. (Consulte "🔒" en la página 19 para obtener más información).

MANUAL DE CIFRADO

La criptografía utiliza una fórmula matemática para traducir un texto simple a una forma ilegible para personas sin conocimiento específico (denominada clave). La criptografía se aplica a datos almacenados así como a datos transmitidos a través de una red.

EL CIFRADO cambia el texto simple a texto cifrado.

EL DESCIFRADO cambia el texto cifrado nuevamente a texto simple.

Por ejemplo:

Este es información secreta, no...

CLAVE DE CIFRADO

5a0 (k\$hQ%...

CLAVE DE DESCIFRADO

Este es información secreta, no...



Revise los terminales de pago para detectar alguna alteración

Costo



Nivel de
complejidad



Mitigación de
riesgos



Los “dispositivos de duplicación” capturan los datos de la tarjeta de sus clientes cuando ingresan a un terminal de pago. Es fundamental que usted y su personal sepan cómo detectar un dispositivo de duplicación. Usted debe verificar periódicamente sus terminales de pago para comprobar que no hayan sido alterados. Lleve un registro de los terminales que fueron verificados, cuándo, quién realizó la verificación y si se encontró algo inusual.

Consulte la PCI Council's guide: [Skimming Prevention: Overview of Best Practices for Merchants](#) (Guía del Consejo de la PCI: Prevención contra la duplicación – Descripción general de las mejores prácticas para los comerciantes)

Manténgase alerta y siga estos pasos:

CREE UNA LISTA de todos los terminales de pago y tome fotografías (de la parte delantera, trasera, cables y conexiones), así sabe el aspecto que se supone deben tener.

BUSQUE SEÑALES OBVIAS de alteración, como sellos rotos en los tornillos o las placas protectoras de acceso, cableado extraño/diferente, o funciones o dispositivos nuevos que no reconoce. La guía de Consejo (mencionada a continuación) puede ser de ayuda.

PROTEJA LOS TERMINALES. Manténgalos fuera del alcance de los clientes cuando no los utilice y oculte las pantallas de la vista del público. Asegúrese de que sus terminales de pago estén protegidos antes de finalizar el día y cerrar su tienda, incluso cualquier dispositivo que lea las tarjetas de pago de sus clientes o acepte sus números de identificación personal (PIN).

CONTROLE LAS REPARACIONES. Permita que únicamente el personal autorizado realice las reparaciones de los terminales de pago, y solo si las prevé. Infórmele a su personal también.

LLAME a su banco comercial o proveedor de terminal de pago inmediatamente si sospecha de algo.



Instale parches provistos por sus proveedores

Costo



Nivel de
complejidad



Mitigación de
riesgos



Generalmente, el software presenta fallas o errores cometidos por los programadores cuando escriben el código, también denominados agujeros de seguridad, errores o vulnerabilidades. Los hackers aprovechan estos errores para irrumpir en su computadora y robar los datos de cuentas. Proteja sus sistemas aplicando los "parches" provistos por los proveedores para arreglar los errores de código. ¡La instalación de parches de seguridad de manera oportuna es fundamental!

PREGÚNTELE a su proveedor o proveedor de servicios cómo le notifica sobre los nuevos parches de seguridad y asegúrese de recibir y leer estos avisos.

¿CUÁLES SON LOS PROVEEDORES QUE LE ENVÍAN PARCHES? Usted puede recibir parches de proveedores de su terminal de pago, aplicaciones de pago, otros sistemas de pago (cajas registradoras, computadoras, etc.), sistemas operativos (Android, Windows, iOS, etc.), software de aplicación (incluido su navegador web) y un software comercial.

ASEGÚRESE de que sus proveedores actualicen sus terminales de pago, sistemas operativos, etc., así son compatibles con los últimos parches de seguridad. Solicítele.

COMERCIANTES DE COMERCIO ELECTRÓNICO. La instalación de parches lo antes posible es muy importante para usted también. Además, esté atento a los parches del proveedor de servicios de pagos. Pregúntele a su proveedor de hosting de comercio electrónico si él aplica los parches a su sistema (y con qué frecuencia). Asegúrese de este actualice el sistema operativo, la plataforma de comercio electrónico o la aplicación web para lograr compatibilidad con los parches más recientes.

SIGA las instrucciones de su proveedor de servicios/ proveedor e instale esos parches lo antes posible.



Utilice socios comerciales de confianza y sepa cómo contactarlos

Costo



Nivel de complejidad



Mitigación de riesgos



Usted utiliza proveedores externos para aplicaciones, dispositivos y servicios relacionados con pagos. Además, es posible que tenga proveedores de servicios con los que comparte datos de la tarjeta, que dan soporte a sus sistemas de pago o los administran, o a los que da acceso a los datos de la tarjeta. Puede llamarlos procesadores, proveedores, terceros o proveedores de servicios. Todos ellos afectan su capacidad de proteger sus datos de tarjeta, de modo que es fundamental que sepa quiénes son y qué tipo de preguntas de seguridad debe hacerles.

SEPA A QUIÉN LLAMAR. ¿Cuál es su banco comercial? ¿Quién más le ayuda a procesar pagos? ¿A quién le compró su software/dispositivo de pago y quién se lo instaló? ¿Quiénes son sus proveedores de servicios?

ANÓTELOS EN UNA LISTA. Ahora que sabe a quién debe llamar, guarde los nombres de contacto y las compañías, números de teléfono, direcciones de sitio web y otros detalles de contacto en un lugar donde los pueda encontrar fácilmente en caso de una emergencia.

CONFIRME LA SEGURIDAD DE SUS PROVEEDORES DE SERVICIOS. ¿Su proveedor de servicios cumple con los requisitos de la PCI DSS? Para los comerciantes de comercio electrónico, es importante que el proveedor de servicios de pago también cumpla con la PCI DSS. Consulte los Recursos en la página 22 para obtener la lista de proveedores de servicios que cumplen con la PCI DSS.

HAGA PREGUNTAS. Una vez que sepa quiénes son sus proveedores externos y qué hacen por usted, hable con ellos para entender cómo protegen los datos de la tarjeta. Utilice [Preguntas para hacerles a sus proveedores](#) que le ayudarán a saber qué preguntar.

COMPRENDA QUÉ SON PROVEEDORES COMUNES. Revise la barra lateral a la derecha para comprender cuáles son los tipos comunes de proveedores o proveedores de servicios con los que quizás trabaje.

PROVEEDORES COMUNES

Consulte la tabla en [Preguntas para hacerles a sus proveedores](#) para obtener más información sobre estos proveedores comunes:

Proveedores de terminal de pagos

Proveedores de aplicación de pago

Instaladores de sistemas de pago (llamados revendedores/integradores)

Proveedores de servicios que realizan procesamiento de pagos o procesamiento o hosting de comercio electrónico

Proveedores de servicios que ayudan a cumplir con el (los) requisito(s) de la PCI DSS (por ejemplo, brindar servicios de antivirus o firewall)

Proveedores de software como servicio



Proteja el acceso interno a sus datos

Costo



Nivel de
complejidad



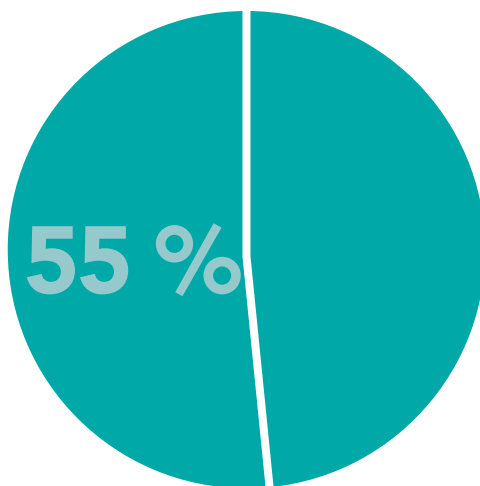
Mitigación de
riesgos



Abuso de privilegios significa una persona que utiliza...

Los privilegios y el acceso de otra persona para obtener acceso a los sistemas o datos a los que dicha persona no tiene la autorización para acceder.

EL ABUSO DE PRIVILEGIO ES EL PRINCIPAL ACCIONAR QUE CONDUCE A FILTRACIONES (APROXIMADAMENTE EL 55 % DE TODOS LOS INCIDENTES INFORMADOS).



Verizon 2015

EL CONTROL DE ACCESO ES LO MÁS

IMPORTANTE. Configure su sistema para otorgar acceso únicamente en función de “la necesidad de saber que tenga la empresa”. Como propietario, usted tiene acceso a todo. Pero la mayoría de los empleados pueden hacer su trabajo con tener acceso solamente a un subconjunto de datos, aplicaciones y funciones.

LIMITE EL ACCESO a los sistemas de pago y a los datos no cifrados de la tarjeta a aquellos empleados que necesitan acceso, y solamente a los datos, aplicaciones y funciones que necesitan para hacer su trabajo.

LLEVE UN REGISTRO. Registre todos los visitantes “detrás del mostrador” de su establecimiento. Incluya nombre, motivo de la visita y nombre del empleado que autorizó el acceso del visitante. Conserve el registro por lo menos un año.

DESECHE LOS DISPOSITIVOS DE FORMA SEGURA.

Pregúntele a su proveedor de sistema de pago o proveedor de servicios cómo eliminar los datos de la tarjeta de forma segura antes de vender o eliminar dispositivos de pago (para que no se puedan recuperar los datos).

COMPARTA ESTA INFORMACIÓN. Proporcióneles esta guía a sus empleados y socios comerciales así están al tanto de lo que se espera.

Considere la posibilidad de darles acceso a los empleados para que registren pagos, pero no para que procesen reintegros o tomen nuevas reservas/pedidos, pero no para acceder a datos de la tarjeta de pago relacionados con pedidos/reservas existentes. Algunos empleados no deberían tener ningún tipo de acceso.



No les facilite a los hackers el acceso a su sistema

Costo



Nivel de complejidad



Mitigación de riesgos



HACKERS = DELINCUENTES

Una de las formas más fáciles que tienen los hackers para irrumpir en su sistema es a través de la gente en quien confía. Usted necesita saber cómo acceden sus proveedores al sistema para asegurarse de que no están dejando ningún agujero para los hackers.

La autenticación de múltiples factores emplea un nombre de usuario y contraseña además de otro factor como mínimo (como una tarjeta inteligente, un dongle* o un código de entrada único).

*un dispositivo portátil que se conecta a una computadora para permitir el acceso inalámbrico, funciones de software, etc.

AVERIGÜE. Pregúntele al proveedor de servicios o proveedor de sistema de pago si utilizan acceso remoto para dar soporte o acceder a su empresa.

PREGUNTE CÓMO LIMITAR EL USO DEL ACCESO REMOTO. Muchos programas de acceso remoto siempre funcionan de forma predeterminada. Reduzca su riesgo. Pregúntele a su proveedor cómo desactivar el acceso remoto cuando no se necesita y cómo activarlo cuando su proveedor o proveedor de servicios específicamente lo solicita.

DESACTÍVELO CUANDO TERMINE.

UTILICE UNA AUTENTICACIÓN SEGURA. Si debe permitir el acceso remoto, solicite autenticación de múltiples factores y criptografía sólida.

ASEGÚRESE DE QUE LOS PROVEEDORES DE SERVICIOS UTILICEN CREDENCIALES EXCLUSIVAS. Cada uno debe usar credenciales de acceso remoto que son únicas para su empresa y que no son las mismas que utilizan para otros clientes.

PIDA AYUDA. Solicítele a su proveedor o proveedor de servicios que le ayude a desactivar el acceso remoto, o (si su proveedor o proveedor de servicios necesita acceso remoto) que le ayude a configurar una autenticación de múltiples factores. Consulte las [Preguntas para hacerles a sus proveedores](#) que le ayudarán a saber exactamente qué preguntar.

Si su proveedor le brinda soporte a un terminal de pago, o soluciona problemas de este, desde la oficina del proveedor (y no desde su ubicación) está utilizando Internet y el software de acceso remoto para hacer esto.

VNC y LogMeIn son ejemplos de productos que su proveedor puede instalar en su terminal y utilizar para brindarle soporte de forma remota.



Utilice un software antivirus

Costo



Nivel de
complejidad



Mitigación de
riesgos



Los sistemas y softwares son extremadamente flexibles y ofrecen una amplia variedad de funciones y características. Los hackers utilizan virus y códigos maliciosos para aprovechar esas características y errores de códigos, así pueden irrumpir en sus sistemas y robar los datos de la tarjeta. El uso de un antivirus actualizado (también denominado software contra malware) le ayuda a proteger sus sistemas.

INSTALE UN SOFTWARE ANTIVIRUS PARA PROTEGER SU SISTEMA DE PAGO. Es fácil de instalar y puede obtenerlo de su comercio minorista de TI o tienda de suministros de su oficina local.

CONFIGURE LA OPCIÓN “ACTUALIZACIÓN AUTOMÁTICA” DEL SOFTWARE, de modo que siempre obtenga la protección más reciente disponible.

ASESÓRESE. Pregúntele a su comercio minorista de TI sobre los productos que recomienda para la protección contra malware/antivirus.

REALICE ANÁLISIS PERIÓDICOS. Realice análisis completos del sistema de forma periódica, ya que sus sistemas pueden haber sido infectados por un nuevo malware que fue lanzado antes de que su software antivirus pudiera detectarlo.



Realice un análisis de vulnerabilidades y arregle los problemas

Costo



Nivel de
complejidad



Mitigación de
riesgos



Todos los días se descubren vulnerabilidades, agujeros de seguridad y errores nuevos. Es sumamente importante que pruebe sus sistemas con acceso a Internet de manera periódica para identificar estos nuevos riesgos y abordarlos lo antes posible. Sus sistemas con acceso a Internet (como muchos sistemas de pago) son los más vulnerables porque los delincuentes los pueden aprovecharse fácilmente, dado que les permiten escabullirse en sus sistemas.

Los proveedores aprobados de escaneo (ASV) del Consejo de la PCI realizan un informe y escaneo de vulnerabilidades externos. Consulte la [List of PCI-Approved Scanning Vendors](#) (Lista de proveedores aprobados de escaneo la PCI.)

ASESÓRESE. Pregúntele a su banco comercial si está asociado con algún proveedor aprobado de escaneo (Approved Scanning Vendor, ASV) de la PCI. También pregúntele a sus proveedores y proveedores de servicios.

HABLE CON UN ASV DE LA PCI. Estos proveedores pueden ayudarle con herramientas que buscan automáticamente su red para detectar vulnerabilidades y le suministran un informe, si, por ejemplo, usted necesita aplicar un parche. La lista del Consejo de la PCI (mencionada a continuación) puede ayudarle a encontrar un proveedor de escaneo.

SELECCIONE UN ESCÁNER. Comuníquese con varios ASV de la PCI para encontrar uno con un programa adecuado para su pequeña empresa.

ABORDE LAS VULNERABILIDADES. Pídale a su ASV que le ayude a corregir problemas que detectó en el escaneo.



Utilice soluciones y terminales de pago seguros

Costo




Nivel de complejidad



Mitigación de riesgos



Una forma segura de proteger mejor su empresa es utilizar soluciones de pago seguras y profesionales capacitados que le ayuden. Aquí le indicamos cómo escoger productos seguros y asegurarse de que están configurados correctamente.

Para ver los terminales de pago de la PCI y lectores de tarjeta seguros que pueden cifrar los datos de la tarjeta, consulte  la página 19.

UTILICE TERMINALES DE PAGO Y DISPOSITIVOS DE INGRESO DE PIN SEGUROS. El Consejo de la PCI aprueba los terminales de pago que protegen los datos del PIN. Asegúrese de que su terminal o dispositivo de pago se encuentra en la [List of PCI Approved PTS Devices \(Lista de dispositivos para la seguridad de la transacción con PIN \(PTS\) aprobados de la PCI\)](#) para equipos que ofrecen la mejor seguridad y son compatibles con “chip de tipo EMV”.

UTILICE UN SOFTWARE SEGURO. Asegúrese de que su software de pago se encuentre en la Lista de [List of PCI Validated Payment Applications \(Aplicaciones de pago validadas de la PCI\)](#).

UTILICE PROFESIONALES CALIFICADOS. Asegúrese de que la persona que instale su aplicación validada según la PA-DSS lo haga de forma correcta y segura. Escoja de la [List of PCI QIRs \(Lista de integradores y revendedores certificados \(QIR\) de la PCI\)](#) de las compañías autorizadas por el Consejo de la PCI para que le ayuden. Pídale a su banco comercial que le ayude a hacer la selección.

CONSULTE ESTA LISTA DE PREGUNTAS PARA EL PROVEEDOR. Utilice [Preguntas para hacerles a sus proveedores](#) que le ayudarán a saber qué preguntarles a sus proveedores y proveedores de servicios.

Sus clientes ingresan los números de identificación personal (PIN) de sus tarjetas de pago en su terminal de pago o dispositivo de entrada de PIN. Es importante utilizar dispositivos seguros para proteger los datos del PIN del cliente.



Proteja su empresa de Internet

Costo	
Nivel de complejidad	
Mitigación de riesgos	

Internet es la principal vía de acceso que utilizan los ladrones de datos para atacar y robar los datos de las tarjetas de sus clientes. Por esta razón, si su empresa está en Internet, todo lo que utilice para los pagos con tarjeta necesita protección adicional.

AÍSLE EL USO. No utilice el dispositivo en el que registra pagos para realizar otra tarea. Por ejemplo, no navegue por la web o revise correos electrónicos o redes sociales desde el mismo dispositivo o computadora que utiliza para realizar transacciones de pago. Cuando necesite hacer algo para su empresa (por ejemplo, actualizar la página de redes sociales de su empresa), utilice otra computadora y no su dispositivo de pago para realizar estas actualizaciones.

PROTEJA SU "TERMINAL VIRTUAL". Si usted ingresa los pagos del cliente por medio de un terminal virtual (una página web a la que accede con una computadora o tableta), minimice su riesgo y no le conecte un lector de tarjetas externo.

PROTEJA LA RED WI-FI. Si su tienda ofrece conexión de Wi-Fi gratis a sus clientes, asegúrese de usar otra red para su sistema de pago (esto se denomina "segmentación de red"). Pídale ayuda a su instalador de red para configurar la red Wi-Fi de forma segura.

UTILICE UN FIREWALL. Un firewall configurado correctamente actúa como un buffer para impedir que los hackers y los softwares maliciosos accedan a sus computadoras e información. Verifique con su proveedor de servicios o proveedor de terminal de pago para asegurarse de que tiene uno y pídale ayuda para configurarlo correctamente.

UTILICE UN SOFTWARE DE FIREWALL PERSONAL O EQUIVALENTE cuando los sistemas de pago no están protegidos por el firewall de su empresa (por ejemplo, cuando se conecta a una red Wi-Fi pública).



Para tener la mejor protección, convierta los datos de su tarjeta en información inutilizable para los delincuentes

Costo



Nivel de complejidad




Mitigación de riesgos



Sus datos son vulnerables cuando se transfieren a su banco comercial y cuando se conservan o almacenan en sus computadoras o dispositivos. La mejor forma de mantenerlos seguros es convirtiéndolos en información inutilizable, incluso si son robados, escondiéndolos o eliminándolos todos juntos cuando ya no son necesarios. Si bien esto puede ser más difícil de implementar, a largo plazo, se puede lograr que la seguridad sea mucho más fácil de manejar.

PREGÚNTELE A SU PROVEEDOR DE SISTEMAS DE PAGO O PROVEEDOR DE SERVICIOS si su terminal de pago utiliza alguna tecnología de cifrado o tokenización.

UTILICE LOS DISPOSITIVOS DE LA PCI QUE CIFRAN LOS DATOS DE LA TARJETA. El Consejo de la PCI aprueba los terminales de pago que protegen los datos del PIN (consulte  en la página 17) y los terminales de pago y "lectores de tarjeta seguros" que también cifran los datos de la tarjeta. Consulte la [List of PCI Approved PTS Devices \(Lista de dispositivos PTS aprobados de la PCI\)](#).

UTILICE SOLUCIONES DE CIFRADO DE LA PCI SEGURAS. Pregunte si el cifrado de su terminal de pago se realiza a través de una solución de cifrado de punto a punto y si se encuentra en la [PCI Validated Payment Applications \(Lista de Soluciones de cifrado de punto a punto \(P2PE\) validadas de la PCI\)](#) del Consejo de la PCI.

ACTUALICE SU SOLUCIÓN. Reduzca su riesgo, considere la posibilidad de obtener un nuevo terminal de pago que utilice ambas tecnologías de cifrado y tokenización para eliminar el valor de los datos de la tarjeta para los hackers.

¿ES UN COMERCIANTE QUE AHORA MIGRA A TERMINALES CON CHIP DE TIPO EMV? Esta es una gran oportunidad para hacer una inversión en un terminal que sea compatible con EMV y que además ofrezca seguridad de cifrado y tokenización adicional.

PREGUNTE. Consulte [Preguntas para hacerles a sus proveedores](#) que le ayudarán con las preguntas que debe hacerle a su proveedor o proveedor de servicios.

Los terminales de pago y los lectores de tarjetas seguros aprobados por la PCI que cifran datos de tarjeta lo hacen usando una tecnología llamada "Intercambio y lectura de datos seguros (Secure Reading and Exchange of Data, SRED)"; pregúntele a su proveedor si su terminal de pago cifra los datos con SRED.



DÓNDE OBTENER AYUDA

Recursos

Listas del Consejo de la PCI

Recurso	Enlace	URL
List of Validated Payment Applications (Lista de aplicaciones de pago validadas)	<i>PCI Council's Validated Payment Applications (Aplicaciones de pago validadas del Consejo de la PCI)</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices (Lista de dispositivos de PTS aprobados)	<i>PCI Council's Approved PTS Devices (Dispositivos de PTS aprobados del Consejo de la PCI)</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors (Lista de proveedores aprobados de escaneo)	<i>PCI Council's Approved Scanning Vendors (Proveedores aprobados de escaneo del Consejo de la PCI)</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers (Lista de integradores/ revendedores calificados)	<i>PCI Council's Qualified Integrators Resellers (Revendedores e integradores calificados del Consejo de la PCI)</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions (Lista de soluciones de P2PE validadas)	<i>PCI Council's P2PE Validated Solutions (Soluciones de P2PE validadas del Consejo de la PCI)</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Listas de las marcas de pago

Recurso	Enlace	URL
Lists of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos)	<i>MasterCard's List of Compliant Service Providers (Lista de proveedores de servicios que cumplen con los requisitos de MasterCard)</i>	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	<i>Visa's Global Registry of Service Providers (Registro mundial de proveedores de servicios de Visa)</i>	http://www.visa.com/splisting/
	<i>Visa Europe's Registered Member Agents (Agentes miembros registrados de Visa Europe)</i>	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS y orientación relacionada

Recurso	Enlace	URL
More about PCI DSS (Más información acerca de la PCI DSS)	<i>How to Secure with PCI DSS (Cómo protegerse con la PCI DSS)</i>	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires (Cuestionarios de autoevaluación de la PCI DSS)	<i>Self-Assessment Questionnaires (Cuestionarios de autoevaluación)</i>	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants (Guía: Prevención contra la duplicación: Descripción general de las mejores prácticas para los comerciantes)	<i>Skimming Prevention: Overview of Best Practices for Merchants (Prevención contra la duplicación: Descripción general de las mejores prácticas para los comerciantes)</i>	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Recursos

Infografía y videos

Recurso	Enlace	URL
Infographic: It's Time to Change Your Password (Infografía: Es momento de cambiar su contraseña)	<i>It's Time to Change Your Password (Es momento de cambiar su contraseña)</i>	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves (Infografía: Combata los delitos informáticos convirtiendo los datos robados en información inutilizable para los ladrones)	<i>Fight Cybercrime by Making Stolen Data Worthless to Thieves (Combata los delitos informáticos convirtiendo los datos robados en información inutilizable para los ladrones)</i>	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Video: Learn Password Security in 2 Minutes (Video: Aprenda sobre la seguridad de las contraseñas en 2 minutos)	<i>Learn Password Security in 2 Minutes (Aprenda sobre la seguridad de las contraseñas en 2 minutos)</i>	https://www.youtube.com/watch?v=FsrOXgZKa7U

Recursos de protección de pagos de la PCI para pequeños comerciantes

Recurso	Enlace	URL
Sistemas de pago comunes	<i>Sistemas de pago comunes</i>	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Preguntas de pequeños comerciantes a los proveedores	<i>Preguntas de pequeños comerciantes a los proveedores</i>	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Glosario para pequeños comerciantes	<i>Glosario para pequeños comerciantes</i>	https://es.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Fuentes

Gallup – *Gallup Poll, October 2015* (Gallup – *Encuesta Gallup, octubre de 2015*)

HM Government - *Small Businesses: What You Need to Know about Cyber Security, UK 2014*
(Gobierno del Reino Unido – *Pequeñas empresas: Lo que necesita saber sobre seguridad cibernética, Reino Unido 2014*)

NCSA – *National Cyber Security Alliance survey, 2012* (NCSA – *Encuesta de la Alianza Nacional para la Seguridad Cibernética, 2012*)

National Small Business Administration, *2014 Year End Economic Report* (NSBA – Asociación Nacional de Pequeñas Empresas, *Informe económico de fin de año 2014*)

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report* (Verizon 2012 – *Informe de Investigaciones de Filtraciones de Datos de Verizon 2012*)

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report* (Verizon 2015 – *Informe de Investigaciones de Filtraciones de Datos de Verizon 2015*)

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report* (PCI de Verizon 2015 – *Informe de Cumplimiento de la PCI de Verizon 2015*)