FORTRA™

GUÍA

Cumplimiento de PCI DSS 4.0

Consejos para evitar el pánico en el último momento

Mantener el Cumplimiento es una tarea difícil, tanto por su alcance como por su aplicación práctica. Las organizaciones tienen que cumplir un amplio abanico de normativas, y su número no deja de aumentar. El Cumplimiento es cada vez más estricto y las empresas e instituciones financieras ahora tienen que aprender e integrar los nuevos requisitos del Estándar de Seguridad de Datos para el Sector de Tarjetas de Pago (PCI DSS) 4.0, a medida que se acerca la fecha límite de implementación en 2024.

Cumplir con un estándar nuevo o actualizado es más fácil decirlo que hacerlo. La realidad es que las empresas están ocupadas con las exigencias cibernéticas cotidianas, y el Cumplimiento a menudo se pospone hasta que se convierte en una necesidad crítica que hay que abordar. Esto ocurre sobre todo en las empresas que necesitan más recursos, tiempo y personal, así como una estrategia global para que la Seguridad y el Cumplimiento sean robustos.

Las carencias de talento y la falta de personal son preocupaciones reales en todos los sectores. Como consecuencia, el tiempo y las personas escasean y las empresas tienden a centrarse en los plazos urgentes en lugar de los proyectos a más largo plazo. Este enfoque puede provocar pánico por el Cumplimiento en el último momento.

Sin embargo, los comercios y las entidades financieras pueden abordar sus operaciones y requisitos de Seguridad cotidianos y, al mismo tiempo, consolidar su Cumplimiento del estándar PCI DSS 4.0. Para ello, pueden adoptar la estrategia de "un solo toque" para resolver dos tareas en una sola acción con el fin de satisfacer las prioridades cotidianas y abordar con eficacia el tránsito al estándar PCI DSS 4.0.

Se trata de hacer las cosas de forma que no haya que volver a hacerlas. Se trata de un proceso de pensamiento por el que, cada vez que se crea un nuevo proceso de Negocio, se debe hacer pensando "¿esto hace que seamos más seguros y cumplamos mejor el estándar PCI DSS 4.0?".

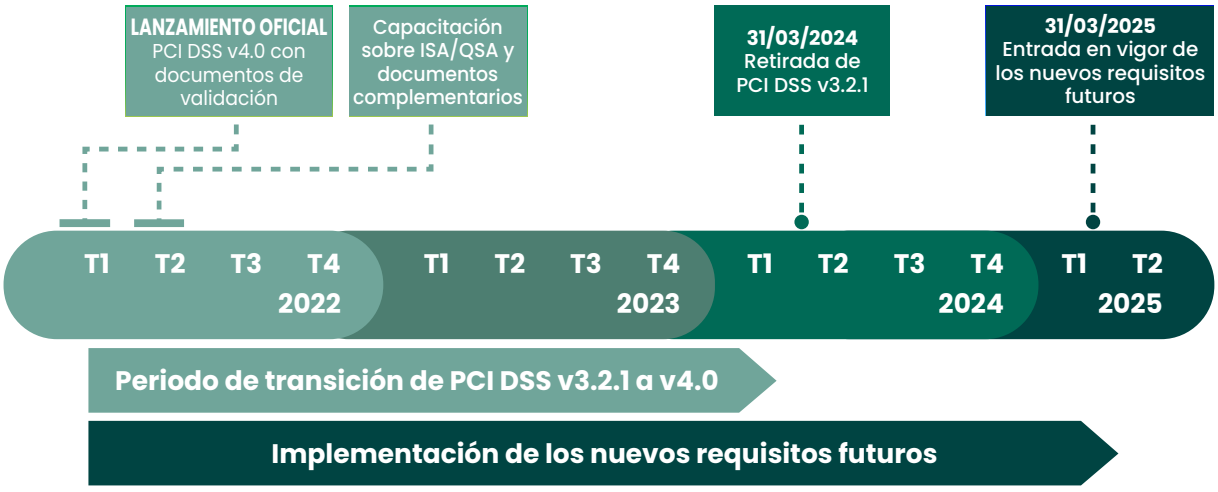
El objetivo de esta guía es ayudarlo a comprender lo que está en juego con el cumplimiento del estándar PCI DSS 4.0 y proporcionarle una hoja de ruta con las prioridades para cumplirlo, protegiendo al mismo tiempo su empresa de los riesgos y amenazas cibernéticos cotidianos.

PCI DSS 4.0: Novedades

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) se desarrolló en 2006 para ayudar a las empresas que procesan, almacenan o transmiten datos de tarjetas de pago a evitar el robo de los datos de los titulares. Aunque se diseñó expresamente para centrarse en los entornos que incluyen datos de cuentas de tarjetas de pago, el estándar PCI DSS también puede proteger contra las amenazas y asegurar otros elementos del ecosistema de pago.

La retirada de la versión 3.2.1 del estándar se solapará con la adopción del estándar PCI DSS 4.0 para suavizar la transición de una versión a otra. Esta coexistencia da a las organizaciones tiempo para familiarizarse con la nueva versión, planear y aplicar los cambios necesarios. El diagrama que figura a continuación, cortesía del Consejo de Estándares de Seguridad de PCI (PCI SSC, por sus siglas en inglés), ofrece un resumen del calendario de implantación del estándar PCI DSS 4.0.

Cronograma de implantación de PCI DSS v4.0



El estándar PCI DSS v3.2.1 permanecerá activo durante dos años tras la publicación de la versión 4.0. Eso da a las organizaciones tiempo para familiarizarse con la nueva versión, planear y aplicar los cambios necesarios.

Hay cuatro razones principales detrás de los cambios incluidos en la versión 4.0:

- Asegurar que el estándar cumpla los requisitos para pagos digitales seguros
- Fomentar la Seguridad como un proceso dinámico continuo
- Reforzar los procedimientos de validación
- Respaldar metodologías adicionales que alcancen los mismos objetivos de Seguridad

Además, la nueva versión incorpora el concepto de enfoque personalizado, que considera que no todos los enfoques de Seguridad son iguales y puede haber muchas formas de alcanzar un objetivo de Seguridad. La versión 4.0 permitirá personalizar los requisitos y los procedimientos de prueba para adaptarlos a este enfoque.

Muchas empresas disponen de soluciones de Seguridad que cumplen el objetivo de Seguridad de un requisito. El enfoque personalizado permite a las empresas mostrar cómo su solución particular cumple el propósito del objetivo de Seguridad y aborda el riesgo con una manera alternativa de cumplir el requisito.

La buena noticia es que los 12 requisitos fundamentales de PCI DSS no cambian con el PCI DSS v4.0, ya que estos son la base crítica para asegurar los datos de las tarjetas de pago. Sin embargo, los requisitos ahora se redactan como afirmaciones basadas en resultados y centradas en la aplicación del control de Seguridad. En muchos de los requisitos, esto se consigue cambiando el lenguaje: de hablar sobre lo que "debe" implementarse, ahora se habla de cuál "es" el resultado para la Seguridad.

Los cambios de mayor alcance afectan a la autenticación y a la encriptación de datos. Con el traslado gradual de la industria de los pagos a la nube, el estándar PCI DSS se centra en aplicar estándares de autenticación más sólidos a los inicios de sesión de acceso a los procesos de pago y control. Los nuevos requisitos incluyen el uso de la autenticación multifactor para todas las cuentas que acceden a los datos de los titulares de tarjetas, no solo para los administradores que acceden al entorno de datos de los titulares de tarjetas. Además, el estándar PCI DSS 4.0 ahora lleva la encriptación de los datos de los titulares de tarjetas a las redes de confianza. Encontrará la lista completa de cambios en la guía resumen de cambios correspondiente.

Un Enfoque Priorizado para el Cumplimiento de PCI DSS 4.0

Por su naturaleza exhaustiva, PCI DSS proporciona una gran cantidad de información sobre Seguridad, tanta que algunas personas responsables de la Seguridad de los datos de las cuentas de pago se preguntarán por dónde empezar. El Consejo de Estándares de Seguridad de PCI ha desarrollado un Enfoque Priorizado del Cumplimiento para ayudar a las organizaciones a comprender cómo reducir el riesgo en una fase más temprana de su camino hacia el Cumplimiento de PCI DSS.

Según la guía, "*el Enfoque Priorizado agrupa todos los requisitos de PCI DSS en seis hitos de Seguridad basados en el riesgo, cuyo objetivo es ayudar a las organizaciones a protegerse de forma incremental contra los factores de mayor riesgo y las amenazas crecientes en su camino hacia el Cumplimiento de PCI DSS*".

El Enfoque Priorizado de PCI DSS incluye seis hitos:

1. **No almacene datos sensibles de autenticación innecesarios y limite la retención de datos del titular de la tarjeta.** Las empresas pueden limitar el impacto de una filtración si no se almacenan datos sensibles de autenticación y otros datos de cuentas.
2. **Proteja los puntos de acceso a los sistemas y redes, y esté preparado para responder a una filtración.**
3. **Aplicaciones de pago seguras.** Las debilidades de estas aplicaciones son un vector común para vulnerar sistemas y obtener acceso no autorizado a los datos de titulares de tarjetas.
4. **Monitoree y controle el acceso a los sistemas.** Tenga claro quién, qué, cuándo y cómo accede al entorno de los datos de titulares de tarjetas.
5. **Proteja los datos de titulares de tarjetas almacenados.** Si almacenar los datos de titulares de tarjetas es una necesidad del Negocio, ponga en marcha controles para proteger estos datos.
6. **Lleve a cabo las demás iniciativas de Cumplimiento y asegúrese de que todos los controles están en su lugar.**

El objetivo de estos hitos es ayudar a las organizaciones a protegerse de forma incremental contra los factores de mayor riesgo y las amenazas durante su camino hacia el cumplimiento del estándar PCI DSS 4.0.

El Enfoque Priorizado y sus hitos proporcionan los siguientes beneficios a todas las organizaciones:

- Un enfoque estructurado para abordar los riesgos por orden de prioridad
- "Victorias rápidas" utilizando un enfoque realista hacia la Ciberseguridad y el Cumplimiento de PCI DSS 4.0
- Planificación financiera y operativa
- Indicadores de progreso objetivos y medibles

Mejores prácticas cotidianas para avanzar hacia el Cumplimiento del estándar PCI DSS 4.0

Cumplir con la versión 4.0 de PCI DSS puede ser difícil, pero ofrece una forma mejorada de mitigar las tácticas avanzadas que los atacantes emplean. En primer lugar, lea el estándar PCI DSS 4.0 y familiarícese con los cambios más significativos que podrían afectar a su proceso de Cumplimiento. Después, empiece a elaborar planes para aplicar los cambios en sus procesos de Ciberseguridad que le mantendrán en el camino del Cumplimiento del estándar PCI DSS 4.0.

Los párrafos a continuación, lo guiarán por los 12 requisitos del estándar y le ofrecerán las mejores prácticas para proteger su organización de las amenazas diarias y, al mismo tiempo, reforzar su Cumplimiento de PCI DSS 4.0. Para obtener información más detallada, consulte los recursos sobre PCI DSS.

Requisito 1: Instalar y mantener controles de Seguridad de la red

Tener firewalls en la red es vital para su Seguridad. Sin embargo, para estar seguro necesita algo más que instalar un firewall en el perímetro de la red de su organización.

1. **Cree una configuración de referencia del firewall:** Antes de implementar la configuración del firewall, documente los ajustes y procedimientos, como la configuración de Seguridad del hardware, las reglas de los puertos o servicios necesarios para el Negocio y la justificación de estas reglas, y tenga en cuenta tanto el tráfico entrante como el saliente.
2. **Pruebe toda la configuración:** Después de implementar la configuración del firewall, pruébela externa e internamente para confirmar que sea correcta.
3. **Limite el tráfico saliente (no solo el entrante):** Con frecuencia, nos preocupamos demasiado por bloquear los puertos de entrada y tenemos que acordarnos de limitar el tráfico de salida desde el interior de la red a lo que sea estrictamente necesario. Esto limita las vías que los atacantes pueden utilizar para filtrar datos.
4. **Configure firewalls en los dispositivos móviles personales:** Instale firewalls personales en las plataformas de computación móviles para que, cuando se conecten a redes no seguras, limiten la superficie de ataque y minimicen la propagación de malware.
5. **Desactive la gestión externa del firewall:** Gestione el firewall únicamente desde su red. Desactive los servicios de gestión externos a menos que formen parte de una infraestructura de firewall gestionada de forma segura.

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

1. **Cambie los ajustes por defecto para reducir las debilidades inherentes:** Los dispositivos vienen con valores de fábrica, como nombres de usuario y contraseñas. Los valores por defecto facilitan la instalación de dispositivos y la asistencia técnica, pero también significan que, originalmente, todos los modelos utilizan el mismo nombre de usuario y contraseña. Si no se modifican los valores por defecto, se proporciona a los atacantes una vía de acceso fácil a su ecosistema. Es vital cambiar los valores por defecto del proveedor en todos los sistemas que acceden a los datos de titulares de tarjetas.
2. **Refuerce el Entorno de Datos de Titulares de Tarjetas (CDE) de acuerdo con las mejores prácticas de la industria:** Todos los sistemas que se usen en el CDE deben reforzarse antes de pasar a producción. El objetivo de solidificar un sistema es eliminar las funciones innecesarias y configurar las necesarias de forma segura. Cada aplicación o dispositivo conectado a un sistema introduce vulnerabilidades. Según el requisito 2.2 de PCI DSS, debe *"abordar todas las vulnerabilidades de Seguridad conocidas y ser coherente con los estándares de refuerzo del sistema aceptados por la industria"*.
3. **Sea coherente y mantenga el inventario actualizado:** Una vez implementado y documentado el refuerzo del sistema, la configuración debe aplicarse a todos los sistemas del entorno de forma consistente. Cuando todos los sistemas y dispositivos del dominio se hayan configurado correctamente, deberá designar a un responsable de mantener el inventario actualizado. De este modo, se pueden identificar y eliminar las aplicaciones y los sistemas cuyo uso no esté aprobado.

Requisito 3: Proteger los datos de cuentas almacenados

1. **Sepa dónde residen sus datos:** Utilice una herramienta de detección de datos para identificar la ubicación de los datos no encriptados y poder eliminarlos o encriptarlos. También ayudan a determinar qué procesos o flujos podrían tener que arreglarse. Los datos de los titulares de tarjetas pueden quedar expuestos fácilmente debido a procesos deficientes o a una mala configuración. Empiece por buscar donde cree que están los datos y, a continuación, investigue todos los lugares donde no deberían estar.
2. **Encripte todos los datos almacenados:** Los datos de tarjetas almacenados deben encriptarse mediante algoritmos aceptados por la industria. Muchas organizaciones poseen, sin saberlo, números de cuenta principales (PAN) sin encriptar. Además de encriptar los datos de las tarjetas, las empresas deben proteger las claves de encriptación. No salvaguardar la ubicación de la clave de encriptación con un proceso de gestión sólido es como dejar la llave de casa en la cerradura de la puerta principal.
3. **Reduzca al mínimo los datos que posee:** No guarde datos que no necesite. Minimice el alcance de PCI DSS y pregúntese si realmente necesita un registro de datos.

Requisito 4: Proteger los datos de los titulares de tarjetas con una encriptación sólida durante la transmisión a través de redes públicas abiertas

1. **Asegure los datos que se transmiten a través de redes abiertas y públicas:** Identifique dónde envía los datos de los titulares de tarjetas. Debe encriptar sus datos mientras se desplazan por redes públicas abiertas.
2. **Deje de utilizar versiones obsoletas de SSL/TLS:** Se sabe que las versiones más antiguas de SSL y TLS tienen vulnerabilidades de Seguridad. Debe dejar de utilizar estos protocolos de encriptación obsoletos a menos que las necesidades del Negocio obliguen a mantener la compatibilidad con versiones anteriores, como el uso de hardware de TPV no compatible con versiones posteriores de TLS seguro.

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

1. **Actualice regularmente el antivirus:** Una gestión vigilante de las vulnerabilidades es la forma más eficaz de reducir proactivamente el área de riesgo y de reducir considerablemente las probabilidades de que los atacantes logren penetrar en sus sistemas y robar datos valiosos. Incluya un software antivirus actualizado como parte de su estrategia de gestión de vulnerabilidades.

Requisito 6: Desarrollar y mantener sistemas y software seguros

1. **Actualice y parchee los sistemas con regularidad:** La aplicación oportuna de las actualizaciones de Seguridad es fundamental para su seguridad. Parchee todos los componentes críticos de su entorno, incluidos los navegadores, firewalls, aplicaciones, bases de datos, terminales de punto de venta y sistemas operativos. Actualice su software de forma constante para cumplir con el requisito 6.3.3 de PCI DSS, que establece que las organizaciones deben "instalar los parches críticos en el plazo de un mes desde su lanzamiento". Recuerde las instalaciones de software críticas, como las aplicaciones de pago con tarjeta de crédito y los dispositivos móviles. Otra forma de mitigación es el escaneado de vulnerabilidades, que proporciona el mejor método para descubrir brechas de Seguridad conocidas que los ciberdelincuentes pueden aprovechar para acceder a una organización y comprometerla.
2. **Establezca procesos de desarrollo de software seguros:** Si desarrolla aplicaciones de pago internamente, debe utilizar procesos de desarrollo estrictos y directrices de codificación segura. Recuerde desarrollar y probar las aplicaciones de conformidad con los estándares aceptados por la industria, como OWASP.
3. **Instale firewalls de aplicaciones web:** El requisito 6.4 de PCI DSS exige monitorear periódicamente, detectar y prevenir los ataques web protegiendo las aplicaciones web públicas con firewalls de aplicación web (WAF). Estas soluciones se especializan en monitorear y bloquear el tráfico web malicioso.

Requisito 7: Restringir el acceso a los componentes del sistema y a los datos de titulares de tarjetas

1. **Restrinja el acceso a datos y sistemas:** Es necesario disponer de un sistema de control de acceso basado en roles (RBAC), con una lista de roles definida y actualizada, que conceda acceso a los datos de titulares de tarjetas según la necesidad de conocerlos. Restringir el acceso ayuda a evitar la exposición de información confidencial a personas no autorizadas.

Requisito 8: Identificar a los usuarios y autenticar el acceso

1. **Establezca políticas de contraseñas fuertes y únicas e implemente un gestor de contraseñas:** Si un nombre de usuario o contraseña no cumple con los requisitos de longitud, unicidad y complejidad, se convierte en una vulnerabilidad. Para hacer frente a los límites y riesgos que plantea la naturaleza humana, considere la posibilidad de implementar un software corporativo de gestión de contraseñas, para que la complejidad de las contraseñas no menoscabe la experiencia del usuario.
2. **Gestión de cuentas robusta:** PCI DSS exige desactivar las cuentas por defecto y tener nombres únicos para las cuentas de usuario y administrador. Colocar más barreras en el camino de un atacante es una mayor protección para una empresa.
3. **Implemente la autenticación multifactor:** Una sola contraseña, por muy segura que sea, no puede ser la única medida de Seguridad. La autenticación multifactor (MFA) es la solución más eficaz para proteger el acceso remoto y es un nuevo requisito del estándar PCI DSS 4.0. Sus métodos de autenticación deben estar fuera de la red principal y ser independientes entre sí. Debe existir una separación física entre los factores de autenticación para que el acceso a un factor no dé acceso a otro. Si un factor se ve comprometido, no afecta a la integridad y confidencialidad de ningún otro factor. Además, el estándar PCI DSS exige la "*incorporación de autenticación multifactor en todos los accesos remotos a la red (tanto de usuarios como de administradores, así como de terceros con fines de soporte o mantenimiento) que se originen fuera de la red de la entidad*".

Requisito 9: Restringir el acceso físico

1. **Controle el acceso físico a sus instalaciones:** Mitigue los riesgos para la Seguridad física aplicando políticas que preserven la Seguridad física on-premise de los activos y datos críticos. Por ejemplo, puede proteger estos activos críticos en unas instalaciones reforzadas. También podría limitar el acceso de personas ajenas a una única entrada monitoreada y exigir que las personas no empleadas lleven distintivos de visitante.
2. **Monitoree los terminales de punto de venta:** Los Negocios que utilicen sistemas de TPV o dispositivos de pago móviles deben mantener una lista actualizada de todos los dispositivos, inspeccionarlos periódicamente y proporcionar la debida capacitación en concienciación al personal que interactúe a diario con los dispositivos de pago con tarjeta.

Requisito 10: Registrar y monitorear todos los accesos

1. **Revise regularmente los registros y las alertas del sistema:** Los sistemas que controlan los registros monitorean la actividad de la red, examinan los eventos del sistema, advierten de actividades sospechosas y registran las acciones de los usuarios que tienen lugar en su entorno. Se requiere la recopilación y transmisión de registros a una ubicación centralizada, a un servidor de registro on-premise o a un servicio de Internet. Para buscar errores, irregularidades o actividades sospechosas que se desvíen de lo habitual, las empresas deben analizar sus registros a diario. Un programa de Seguridad más eficaz y una respuesta más rápida a las incidencias de Seguridad son las dos ventajas de un monitoreo diligente de los registros. Además de demostrar su compromiso con el Cumplimiento de las normas PCI DSS, el análisis de registros y el monitoreo periódico también ayudan a frustrar las amenazas entrantes y salientes.

Requisito 11: Probar periódicamente la Seguridad de los sistemas y las redes

1. **Reconozca su entorno, busque regularmente vulnerabilidades y realice pentests:** Los atacantes pueden obtener acceso a un entorno a través de puntos débiles en navegadores, clientes de correo electrónico, software de TPV, sistemas operativos e interfaces de servidor. Muchos de los puntos débiles y vulnerabilidades descubiertos recientemente pueden solucionarse antes de que los atacantes se aprovechen de ellos mediante la instalación de actualizaciones y parches de Seguridad del sistema en entornos que almacenan información confidencial o datos de titulares de tarjetas. Para encontrar las vulnerabilidades y repararlas, resulta útil contar con un método de escaneo de vulnerabilidades. Los tests de código y los pentests independientes pueden revelar muchos de los puntos débiles que se encuentran con frecuencia en el código de las aplicaciones internas personalizadas. Los pentests y el escaneo de vulnerabilidades se complementan entre sí para promover el máximo nivel de Seguridad de red. Estos escaneos y tests son las mejores líneas de defensa a la hora de identificar los puntos débiles para que las empresas puedan solucionarlos antes de su implementación.

Requisito 12: Respaldar la Seguridad de la información con políticas y programas

1. **Documente y actualice periódicamente todas las prácticas de Seguridad empresarial:** Todos los empleados deben tener fácil acceso a las políticas escritas. En caso de infracción, la documentación podría ayudar a proteger a su empresa de posibles responsabilidades. Las políticas y los procedimientos de Seguridad que se registran de forma completa y precisa permiten ver a los investigadores forenses las medidas de Seguridad de su empresa, y demuestran su proactividad y compromiso con la Seguridad. Las empresas deben actualizar periódicamente la documentación de sus medidas y acciones de Seguridad para cumplir con el estándar PCI DSS 4.0.
2. **Establezca un proceso de evaluación de riesgos:** PCI exige que todas las entidades lleven a cabo una evaluación anual de los riesgos que identifique los recursos clave, las amenazas, los puntos débiles y los peligros. Mediante esta actividad las organizaciones pueden identificar, organizar y gestionar amenazas a la Seguridad de la información. Clasificar o puntuar las amenazas identificadas es uno de los componentes de la evaluación de riesgos, que ayudará a determinar qué vulnerabilidades se deben abordar en primer lugar y a establecer las prioridades. Clasificar, evaluar y mitigar metódicamente los riesgos permite reducir las probabilidades de que un atacante acceda a sus sistemas, los dañe y, eventualmente, detener el ataque.
3. **Cree y pruebe el plan de respuesta ante incidentes:** Debe prepararse para las repercusiones de una filtración de datos. Es su responsabilidad mantener el control del evento, minimizar los daños a los clientes, reducir los costos relacionados con una filtración de datos, comunicarse adecuadamente con las distintas autoridades de conformidad con las distintas normas y estándares, y salvaguardar su empresa. Una estrategia eficaz de respuesta ante incidentes puede reducir los efectos de las filtraciones, las multas y la publicidad negativa, y acelerar la vuelta a la normalidad.
4. **Proporcione entrenamiento en concientización de Seguridad a todos sus empleados:** La mayoría de las filtraciones pueden vincularse a un error humano. Aunque muchos empleados no tienen mala intención, a menudo olvidan las mejores prácticas de Seguridad o no saben con certeza cómo se espera que actúen. Por desgracia, muchos criminales se aprovechan de los errores humanos para obtener información privada. Deben darse directrices específicas a los empleados, así como una capacitación continua. Se les debe recordar el valor de la Seguridad mediante un programa de concientización de Seguridad, que incluya una capacitación frecuente e información sobre las nuevas políticas y procedimientos de Seguridad.

Reflexiones finales

Aún queda tiempo hasta la fecha límite de 2024 para el cumplimiento del estándar PCI DSS 4.0. Empiece pronto para hacer la transición correctamente. No espere hasta 2024 para empezar a cambiar a PCI DSS 4.0. Reparta el esfuerzo y cambie a PCI DSS 4.0 gradualmente.

Piense en sus necesidades futuras e incorpórelas a su estrategia organizativa y a su programa de Seguridad, con el fin de emplear su tiempo eficazmente. Céntrese en los aspectos que sean beneficiosos para la organización a muy largo plazo.

Cómo Fortra puede ayudarlo

El porfolio de Ciberseguridad y Cumplimiento de Fortra ofrece una amplia gama de soluciones y servicios para ayudar a las empresas a cumplir los requisitos del estándar PCI DSS 4.0 y satisfacer las exigencias diarias de protección de la empresa frente a los riesgos y amenazas. El cuadro a continuación asocia los requisitos del estándar PCI DSS 4.0 con las soluciones de Fortra.

Requisito de PCI DSS 4.0	Solución de Fortra
Requisito 1 Instalar y mantener controles de Seguridad de la red	
Requisito 2 Aplicar configuraciones seguras	La funcionalidad de gestión de la configuración de Seguridad Fortra's Tripwire Enterprise permite a las empresas monitorear la configuración de las redes, los servidores, los firewalls y todos los demás componentes.
Requisito 3 Proteger los datos de cuentas almacenados	Con el producto Fortra's Digital Guardian Enterprise DLP, los clientes pueden aplicar políticas de PCI predefinidas para monitorear y bloquear la salida de información crediticia por diversos puntos de salida habituales. Los dispositivos Fortra's Digital Guardian Network DLP inspeccionan todo el tráfico de la red, aplican políticas preconfiguradas para PCI y otras necesidades de cumplimiento con el fin de proteger los datos.
Requisito 4 Proteger los datos de los titulares de tarjetas con una encriptación sólida durante la transmisión a través de redes públicas abiertas	Fortra's GoAnywhere MFT es una Solución de Transferencia Segura de Archivos que ayuda a los usuarios a que sus transferencias de información confidencial cumplan con el estándar PCI DSS. Fortra's Secure Collaboration protege los archivos que contienen información PII y PCI confidencial, sin importar dónde o cómo se compartan. Las organizaciones pueden encriptar y controlar el acceso a los datos de titulares de tarjetas, así como hacer un seguimiento y una auditoría de los datos, y revocar el acceso a los mismos.
Requisito 5 Proteger los sistemas y las redes de software malicioso	Fortra's Powertech Antivirus protege sus servidores frente a numerosas variantes de virus, malware, ransomware, y más otras.
Requisito 6 Desarrollar y mantener sistemas y software seguros	Fortra's Beyond Security ayuda a detectar las vulnerabilidades de las aplicaciones en una fase temprana del proceso de desarrollo con soluciones de Tests Dinámicos de Seguridad de las aplicaciones (DAST) y Tests Estáticos de Seguridad de las Aplicaciones (SAST). Las soluciones de gestión de las vulnerabilidades de Fortra ayudan a identificar y priorizar las vulnerabilidades del entorno para cerrar las brechas de Seguridad antes de que los atacantes las encuentren. Las capacidades de gestión de la configuración de Fortra's Tripwire Enterprise ayudan a detectar cambios no planificados en el entorno para proteger la integridad del sistema. Fortra's Alert Logic MDR Essentials cuenta con herramientas de evaluación y gestión de la exposición y, mediante un escaneado externo, de red y basado en agentes, elabora una vista integral de las exposiciones dentro de los entornos de IT on-premise y en la nube. Fortra's Alert Logic es un proveedor de escaneado aprobado por la PCI. Fortra's Alert Logic Managed WAF protege las aplicaciones web mediante la detección y prevención continua de los ataques web.
Requisito 7 Restringir el acceso a los componentes del sistema y a los datos de titulares de tarjetas	Fortra's Core Security Access Assurance Suite ayuda a identificar y gestionar el acceso en toda la organización con una única interfaz. Core Privileged Access Manager (BoKS) ayuda a controlar el acceso y los privilegios a sistemas e información críticos.
Requisito 8 Identificar a los usuarios y autenticar el acceso	Fortra's Core Password es una solución de autoservicio líder para la gestión segura de contraseñas que cuenta con diversas opciones de acceso, una sólida integración con el servicio de asistencia técnica y la capacidad de aplicar políticas de contraseñas coherentes en cualquier sistema, aplicación o portal web.

Requisito de PCI DSS 4.0	Solución de Fortra
Requisito 9 Restringir el acceso físico	
Requisito 10 Registrar y monitorear todos los accesos	Fortra's Tripwire LogCenter es un motor de correlación con funciones de recopilación, análisis y entrega centralizada de registros. El servicio Fortra's Alert Logic MDR Professional incluye funciones de gestión, almacenamiento y análisis de registros que detectan actividades sospechosas o maliciosas en el punto de entrada mediante análisis avanzados, como UBAD, y clasificados por un analista del SOC cuando proceda. Alert Logic Health Console y Network Health View monitorean y notifican el estado de los dispositivos de seguridad Alert Logic.
Requisito 11 Probar periódicamente la Seguridad de los sistemas y las redes	Las capacidades de gestión de la integridad de Fortra's Tripwire Enterprise ofrecen una imagen clara de cuándo y dónde se realizaron cambios. Fortra es un proveedor de escaneado aprobado (ASV) por la PCI y sus soluciones de gestión de vulnerabilidades ayudan a realizar evaluaciones exhaustivas de la Seguridad para poder priorizar los riesgos más importantes para una organización. Fortra's Alert Logic MDR Essentials cuenta con herramientas de evaluación y gestión de la exposición y, mediante un escaneado externo, de red y basado en agentes, elabora una vista integral de las exposiciones dentro de los entornos de IT on-premise y en la nube. Fortra's Alert Logic es un proveedor de escaneado aprobado por la PCI. Core Impact, de Fortra's Core Security, ayuda a realizar pentests avanzados de forma eficaz. Con automatización guiada y exploits certificados, le permite comprobar su entorno de forma segura utilizando las mismas técnicas que los adversarios actuales.
Requisito 12 Respaldar la Seguridad de la información con políticas y programas	Fortra's Terranova Security ofrece un enfoque centrado en las personas, específico, atractivo y práctico para la capacitación en concienciación sobre la Seguridad, e incluye un módulo de capacitación específico para PCI DSS.

Si no tiene capacidad para gestionar todas estas actividades, nuestros equipos de servicios gestionados de Tripwire y AlertLogic pueden actuar como una extensión de su equipo para reducir sus riesgos de Seguridad y simplificar el cumplimiento del estándar PCI DSS 4.0.

Si desea obtener más información sobre cómo Fortra puede ayudarlo a cumplir con el estándar PCI DSS 4.0,consulte nuestros recursos sobre PCI adicionales o contacte con nosotros. Será un placer escucharlo y ver cómo podemos ayudarlo.

FORTRA™

Fortra.com

Sobre Fortra

Fortra es una compañía de Ciberseguridad como ninguna otra. Creamos un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com/es.

(fta-corp-wp-0324-r2-hm)