Payment Card Industry (PCI)

Marco de Seguridad del Software

Ciclo de Vida del Software Seguro
Requisitos y Procedimientos de Evaluación

Versión 1.1

Febrero de 2021

Cambios en los Documentos

Fecha	Versión	Descripción
Enero de 2019	1.0	Primera divulgación
Febrero de 2021	1.1	Actualización de la v1.0 para abordar los errores y alinearse con los cambios en la *Guía del Programa de SLC* Seguro para respaldar la expansión del programa. Véase el *Marco de Seguridad del Software; Resumen de los Cambios de los Requisitos del Ciclo de Vida del Software Seguro y los Procedimientos de Evaluación de la Versión 1.0 a la 1.1 para* acceder a la descripción de los cambios.

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Índice de Contenido

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Introducción

Este documento, Requisitos del *Ciclo de Vida del Software de PCI (Secure SLC) y los Procedimientos de Evaluación* (en adelante denominado "Norma SLC de Seguridad de PCI"), proporciona una base de requisitos de seguridad con los correspondientes procedimientos de evaluación y orientación para ayudar a los proveedores de software a diseñar, desarrollar y mantener un software seguro a lo largo del ciclo de vida de dicho software.

La Norma SLC de Seguridad de PCI ha sido creada para ser utilizada como parte del Marco de Seguridad del Software de PCI. En este marco, los proveedores de software que deseen validar sus prácticas de gestión del ciclo de vida del software según esta *Norma SLC* de Seguridad de PCI tienen la opción de hacerlo. Para información adicional sobre la validación de Norma SLC de Seguridad de PCI, consulte la *Guía del Programa SLC seguro de PCI.*

Terminología

En el glosario de términos, abreviaturas y acrónimos del Marco de Seguridad del *Software de PCI, disponible en la biblioteca de documentos de PCI SSC, se encuentra la lista de términos, abreviaturas e iniciales aplicables*: https://www.pcisecuritystandards.org/document_library.

Adicionalmente, las definiciones de la terminología general de PCI aparecen en el *glosario de PCI* en el sitio web de PCI SSC en: https://www.pcisecuritystandards.org/pci_security/glossary.

Requisitos del Ciclo de Vida del Software Seguro de PCI

Los requisitos de seguridad definidos en la Norma SLC de Seguridad de PCI (en adelante, "Requisitos SLC de Seguridad de PCI ") amplían los modelos tradicionales del ciclo de vida del desarrollo de software (SDLC) al introducir conceptos y procesos de seguridad a lo largo de todo el ciclo de vida del software, incluyendo las fases de diseño, desarrollo, implantación y mantenimiento. Los conceptos de seguridad descritos en este documento pretenden ayudar a los proveedores de software a proteger los datos sensibles, minimizar las vulnerabilidades y defender el software de ataques a lo largo de todo su ciclo de vida.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Alcance de los requisitos

Los requisitos del SLC seguro de PCI se aplican a los procesos, la tecnología y el personal del proveedor de software que participan en el diseño, desarrollo, implantación y mantenimiento de los productos y servicios de software del proveedor, incluyendo entre otros, los siguientes:

- Las políticas y procesos que rigen la forma en la cual el proveedor de software gestiona su software a lo largo del ciclo de vida del mismo.
- Las herramientas, tecnologías y técnicas utilizadas por el proveedor de software en el desarrollo y la gestión de su software.
- Los métodos y tecnologías de prueba de software utilizados por el proveedor de software y los resultados de dichas pruebas.
- Todas las personas que participan en la gestión del software del proveedor de software, incluyendo al personal del proveedor que aplique y a los colaboradores de terceros.
- Todos los procesos que apoyan las actividades de la gestión del ciclo de vida del software del proveedor, incluyendo la gestión de cambios, la gestión de vulnerabilidades y la gestión de riesgos.
- La metodología de la versión del software del proveedor.
- Toda la orientación que el proveedor de software debe proporcionarle a sus clientes y a las demás partes interesadas para garantizar que los clientes sepan cómo implementar y configurar su software de forma segura.
- Todas las comunicaciones del proveedor de software para las partes interesadas.

Algunos proveedores de software pueden tener varios productos de software cubiertos por diferentes programas de gestión del ciclo de vida del software. Antes de la evaluación de los requisitos de SLC seguro de PCI, los proveedores de software deben identificar los productos del software y los programas de gestión del ciclo de vida del software asociados que se incluirán en la evaluación. Para obtener mayor información en la definición del alcance de la evaluación del SLC Seguro, consulte la guía del *programa SLC seguro de PCI.*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Enfoque de los Requisitos basado en los Objetivos

Existen muchas metodologías y marcos de gestión del ciclo de vida del software sólidos y seguros que, cuando son aplicados e implementados correctamente, pueden producir un software seguro[1]. Reconociendo esto, el Marco de Seguridad del Software de PCI ha adoptado un enfoque "basado en objetivos" para definir los requisitos de SLC seguro de PCI. Este enfoque reconoce que no existe un método "único" para lograr la seguridad del software, y que los proveedores de software necesitan flexibilidad para determinar las prácticas y los métodos de gestión del ciclo de vida del software seguro más apropiado para abordar sus riesgos empresariales y de su software específico.

Para que este enfoque sea exitoso, los proveedores de software deben contar con una sólida práctica de gestión de riesgos como parte integral de sus procesos operativos "habituales". Los controles de seguridad específicos necesarios para cumplir con ciertos requisitos de esta norma —, por ejemplo, los elementos de datos adicionales identificados por el proveedor de software como datos sensibles[2] —, dependerán de las prioridades y procesos de gestión de riesgos del proveedor de software. Si bien este enfoque le proporciona al proveedor de software la flexibilidad necesaria para implementar los controles de seguridad adecuados en función del riesgo identificado, el proveedor de software debe poder demostrar cómo los controles implementados están respaldados por los resultados de sus prácticas de gestión de riesgos. Sin una práctica sólida de gestión de riesgos y sin pruebas que respalden la toma de decisiones basada en el riesgo, la adhesión a los requisitos de SLC seguro de PCI puede ser difícil de validar.

Cuando un requisito de SLC seguro de PCI no define un nivel específico de rigor o una frecuencia mínima para las actividades periódicas o recurrentes, — por ejemplo, la frecuencia requerida con que la cual el proveedor de software debe revisar el rendimiento de la estrategia de seguridad desempeño —, el proveedor de software puede definir el nivel de rigor o la frecuencia según sea apropiado para su negocio. El rigor y la frecuencia definidos por el proveedor de software deben estar respaldados por las evaluaciones de riesgo documentadas y las decisiones de gestión de riesgos que se generen. El proveedor de software debe poder demostrar que su implementación proporciona una garantía continua de que las actividades son efectivas y que cumplen con todos los requisitos de seguridad aplicables.

También es importante reconocer la necesidad de que los proveedores de software entiendan todos los requisitos de seguridad de este documento y consideren la forma en que los controles y procesos de seguridad del software del proveedor funcionan en conjunto para satisfacer los requisitos de seguridad en lugar de centrarse en un solo requisito de forma aislada.

[1] Algunos ejemplos de otras metodologías y marcos de gestión del ciclo de vida del software seguro incluyen los trabajos del NIST, la ISO, SAFECode, Synopsis (BSIMM) y OWASP (OpenSAMM). Consulte estas fuentes para obtener mayor información sobre sus metodologías.

[2] Consulte el *Glosario de Términos, Abreviaturas y Acrónimos del Marco de Seguridad del Software* PCI para obtener la definición de datos confidenciales.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Resumen de los Requisitos

Los requisitos de SLC seguro de PCI están organizados en cuatro secciones principales:

1. Marco de Seguridad del Software
2. Ingeniería de Software Seguro
3. Software Seguro y Gestión de Dato
4. Comunicaciones de Seguridad

Dentro de cada una de las secciones definidas anteriormente, los requisitos de SLC seguro de PCI se subdividen en los siguientes componentes:

- **Objetivos de control** - Los resultados de seguridad que deben alcanzarse. Aunque todos los objetivos de control deben cumplirse para ser validados según esta *Norma SLC de Seguridad de PCI*, los proveedores de software pueden definir los controles, herramientas, métodos y técnicas específicos que utilizan para cumplir todos los objetivos de control.
- **Requisitos de Pruebas** - Las actividades de validación que debe realizar un evaluador para confirmar si se ha cumplido un objetivo de control específico. Si un evaluador determina que los métodos de prueba alternativos son apropiados para validar un objetivo de control particular, este debe justificar y documentar su enfoque de prueba como se describe en la sección Requisitos de Prueba y Procedimientos de Evaluación.
- **Orientación** - Información adicional para ayudar a los proveedores de software y a los evaluadores a comprender mejor la intención de cada objetivo de control y cómo podría cumplirse dicho objetivo. La orientación puede incluir las mejores prácticas a tomar en cuenta, así como ejemplos de controles o métodos que, si se aplican correctamente, podrían lograr que se alcance el objetivo de control. Esta guía no pretende excluir otros métodos que el proveedor de software pueda utilizar para cumplir con un objetivo de control, no sustituye ni modifica el objetivo de control al cual se refiere.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Requisitos de Prueba y Procedimientos de Evaluación

Para facilitar la validación de las prácticas de gestión del ciclo de vida del software del proveedor, los proveedores de software deben presentar pruebas adecuadas que confirmen que han cumplido con los objetivos de control definidos en esta norma. Los requisitos de prueba identificados para todos los objetivos de control describen las actividades que se espera realizar para validar si el proveedor de software ha cumplido con el objetivo. Cuando en un objetivo de control o en un requisito de prueba se especifican sub-apartados, cada apartado debe cumplirse como parte de la validación. Además, cuando se utilizan términos como "periódico", "apropiado" y "razonable" en el requisito de prueba, es responsabilidad del proveedor de software definir y defender sus decisiones respecto a la frecuencia, solidez y madurez de los controles o procesos implementados.

Los Requisitos de Pruebas suelen incluir las siguientes actividades:

- **Análisis:** El evaluador valora de forma crítica la evidencia en los datos. Algunos ejemplos comunes de evidencias son los documentos de diseño y arquitectura de software (electrónicos o físicos), el código fuente, los archivos de configuración y metadatos, los datos de seguimiento de errores y otros resultados de los sistemas de desarrollo de software, y también los resultados de las pruebas de seguridad.
- **Observa:** El evaluador observa una acción o detecta algo en el entorno. Algunos ejemplos de los temas que hay que observar son el personal que realiza tareas o procesos, los componentes del software o del sistema que realizan una función o responden a datos de entrada, las configuraciones o ajustes del sistema, las condiciones ambientales y los controles físicos.
- **Entrevista:** El evaluador conversa con el personal de manera individual. El propósito de las entrevistas puede incluir el análisis de cómo se realiza la actividad, si la actividad se lleva a cabo según lo definido, y si el personal tiene algún conocimiento o comprensión particular de las políticas, procesos, responsabilidades o conceptos aplicables.

Los requisitos de las pruebas les proporcionan tanto a los vendedores de software como a los evaluadores un entendimiento común de las actividades de validación que se espera que ellos se realicen. Los elementos o procesos específicos que se examinen u observen y el personal que se entreviste deben ser apropiados para el objetivo de control que se está validando, así como para la estructura organizativa, la cultura y las prácticas empresariales propias de cada proveedor de software.

Al documentar los resultados de la evaluación, el evaluador identifica las actividades de prueba realizadas y el resultado de cada actividad. Aunque se espera que un evaluador desarrolle todos los requisitos de prueba identificados para todos los objetivos de control, también puede ser posible que un objetivo de control se valide utilizando diferentes métodos de prueba o métodos adicionales. En estos casos, el evaluador debe documentar y justificar por qué se han utilizado otros métodos de prueba y cómo esos métodos proporcionan al menos el mismo nivel de garantía que se habría logrado utilizando los requisitos de prueba definidos en esta norma.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Muestreo

Cuando proceda, el evaluador podrá utilizar el muestreo como parte del proceso de prueba. Las muestras deben ser una selección representativa de las personas, los procesos y las tecnologías cubiertas por la evaluación de SLC seguro de PCI. El tamaño de la muestra debe ser lo suficientemente grande como para que el evaluador tenga la seguridad de que la muestra refleja con exactitud la población total y que los controles se aplican como es esperado

En todos los casos en los cuales las conclusiones del evaluador se basen en una muestra representativa y no en el conjunto total de los elementos aplicables, el evaluador deberá señalar explícitamente este hecho, detallar los elementos elegidos como muestra para las pruebas y justificar la metodología de muestreo utilizada.

Proveedores de Servicios de Terceros

Los proveedores de software a menudo dependen de proveedores de servicios externos para ciertas funciones de la gestión del ciclo de vida del software, por ejemplo, para el desarrollo del software (excluyendo el uso de código abierto), la realización de revisiones del código u otras pruebas del software del proveedor de software, el alojamiento de las plataformas de desarrollo o la entrega del software del proveedor de software, o la integración e instalación de los productos del proveedor de software.

Cuando un servicio de terceros pueda afectar las prácticas de gestión del ciclo de vida del software del proveedor de software o la seguridad del software del proveedor de software, será necesario identificar e implementar los requisitos de SLC seguro de PCI aplicables para ese servicio. El proveedor de software y el proveedor de servicios tendrán que identificar qué funciones de la gestión del ciclo de vida del software están siendo afectadas por el proveedor de servicios e identificar qué requisitos de SLC seguro de PCI son responsabilidad del proveedor de servicios y cuáles son responsabilidad del proveedor de software.

Se espera que el proveedor de software cuente con los procesos para gestionar los riesgos asociados a los proveedores de servicios de terceros, incluyendo (según corresponda para cada servicio):

- Realizar la debida diligencia antes de la contratación;
- Definir claramente las responsabilidades de seguridad;
- Verificación periódica del cumplimiento de las responsabilidades acordadas; y
- Un acuerdo por escrito para garantizar que ambas partes entienden y reconocen sus responsabilidades en materia de seguridad.

Aunque la responsabilidad final de la seguridad del software recae en el proveedor de software, se les puede exigir a los proveedores de servicios que demuestren el cumplimiento de los requisitos de SLC seguro de PCI aplicables en función del servicio prestado. El prestador de servicios puede hacerlo de la siguiente manera

(a) Realizando su propia evaluación de SLC seguro de PCI para los productos o servicios aplicables que son proporcionados al proveedor de software, y proporcionando pruebas al proveedor de software que demuestren su conformidad con los requisitos aplicables del SLC Seguro para ese producto o servicio; o

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

(b) Haciendo que los productos o servicios aplicables se incluyan en la evaluación de SLC seguro de PCI del proveedor de software, y permitiendo que el asesor del proveedor de software evalúe si el producto o servicio cumple con los requisitos aplicables de SLC seguro de PCI.

Las pruebas aportadas por los proveedores de servicios deben ser suficientes para verificar que el alcance de la evaluación de SLC seguro de PCI del proveedor de servicios cubre los servicios aplicables a las prácticas de gestión del ciclo de vida del software del vendedor, y que se validaron los requisitos pertinentes de SLC seguro de PCI. El tipo específico de pruebas que se aporten dependerá de cómo se gestionen las evaluaciones. Por ejemplo, si el proveedor de servicios se somete a su propia evaluación de SLC seguro de PCI, el Informe de Cumplimiento (ROC por sus siglas en inglés) resultante podría proporcionar parte o toda la información que necesita el evaluador del proveedor de software para validar los requisitos de SLC seguro de PCI aplicables. Si el servicio se incluye en la evaluación de SLC seguro de PCI del proveedor de software, las pruebas proporcionadas estarían determinadas por los objetivos de control que se evalúan y los requisitos de prueba para dichos objetivos de control.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Requisitos de SLC Seguro

Gobierno de Seguridad del Software

Se establece un programa formal de gestión de seguridad del software para reflejar el compromiso del proveedor de software con la creación de software seguro y la protección de cualquier dato y recurso confidencial almacenado, procesado o transmitido por ese software.

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 1: Responsabilidad y Recursos de Seguridad El equipo directivo del proveedor de software establece la responsabilidad y autoridad formal para la seguridad de los productos y servicios del proveedor de software. El proveedor de software asigna recursos para ejecutar la estrategia y se asegura de que el personal esté debidamente capacitado.		
1.1 La responsabilidad general por la seguridad de los productos y servicios del proveedor de software la asigna el equipo directivo del proveedor.	**1.1** El evaluador examinará las evidencias suministradas por el proveedor y entrevistará a la persona o personas que tengan asignada la responsabilidad general de la seguridad de los productos y servicios del proveedor para confirmar lo siguiente: • La responsabilidad de garantizar la seguridad de los productos y servicios del proveedor de software se la asigna formalmente a una persona o equipo de la alta gerencia del proveedor de software. • Las responsabilidades incluyen mantener a la alta gerencia informada de las actualizaciones de seguridad, problemas y otros asuntos relacionados con la seguridad de los productos y servicios del proveedor de software. • Se proporcionan actualizaciones a la alta gerencia al menos una vez al año acerca del rendimiento y los cambios en la política y estrategia de seguridad del software del proveedor descrita en el Objetivo de Control 2.	La asignación formal de responsabilidades por parte del equipo directivo del proveedor de software garantiza la visibilidad a nivel estratégico y la influencia sobre las prácticas de seguridad del software del proveedor. La alta gerencia suele representar a las personas o equipos que tienen la responsabilidad y la autoridad para tomar decisiones empresariales estratégicas para la organización del proveedor de software. En muchos casos, los equipos de alta gerencia están formados por los miembros del equipo ejecutivo, como el Director General (CEO por sus siglas en inglés), el Director Financiero (CFO por sus siglas en inglés), el Director de Tecnología (CTO por sus siglas en inglés), el Director de Información (CIO por sus siglas en inglés), el Director de Riesgos (CRO por sus siglas en inglés) o que ejerzan funciones similares, aunque no es el caso en todas las organizaciones. La estructura diferenciada del equipo gerencial viene determinada en última instancia por el proveedor de software. La asignación de la responsabilidad general del programa de seguridad del software del proveedor debe incluir la autoridad para hacer cumplir y ejecutar la estrategia de seguridad del software de la organización. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
		Sin la debida autoridad, los responsables de la seguridad de los productos y servicios del proveedor de software no pueden responsabilizarse dentro de lo razonable, por garantizar que se siga la estrategia de seguridad de la organización. Los responsables de la seguridad del software del proveedor deben presentar a la alta gerencia, las actualizaciones periódicas del estado del programa de seguridad del software del proveedor y del rendimiento de su estrategia. Esto le permite a la alta gerencia asegurarse de que la estrategia se prioriza y se dota de los recursos adecuados, y de que los cambios necesarios como resultado de su rendimiento sean aprobados a tiempo. Las evidencias para apoyar este objetivo de control podrían incluir descripciones de los puestos de trabajo, organigramas, presentaciones, grabaciones de audio, actas de las reuniones de la alta gerencia, informes, correos electrónicos, comunicaciones formales de la alta gerencia al resto de la organización, o cualquier otro registro que refleje claramente la asignación formal de responsabilidad y autoridad, y las comunicaciones entre la alta gerencia y los responsables del programa de seguridad del software del proveedor en relación con el rendimiento del programa.
1.2 Se asignan las responsabilidades de seguridad del software.	**1.2.a** El evaluador examinará la evidencia suministrada por el vendedor para confirmar lo siguiente: • Que las responsabilidades de seguridad del software están claramente definidas y son asignadas a los individuos o equipos apropiados, incluyendo el personal de desarrollo de software. • Que la asignación de responsabilidades para garantizar la seguridad de los productos y servicios del proveedor de software abarca todo el ciclo de vida del software.	Que las personas (incluyendo el personal de terceros) que participen en el diseño, desarrollo, pruebas y el mantenimiento de los productos y servicios del proveedor de software deben tener la responsabilidad de garantizar que el software se diseñe y mantenga de acuerdo con la estrategia de seguridad del proveedor de software y todos los requisitos de seguridad aplicables, incluyendo los requisitos específicos del software. Que las responsabilidades puedan ser asignadas a un individuo, a un grupo, o a una función; sin embargo, los individuos que hayan sido asignados a un grupo o a una función en particular deben *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	1.2.b El evaluador entrevistará a una muestra de entre las personas responsables, incluyendo al personal de desarrollo de software, para confirmar que conocen y comprenden claramente sus responsabilidades en materia de seguridad del software.	entender claramente cómo esas responsabilidades de seguridad del software afectan sus funciones laborales individuales, las expectativas de seguridad de la organización y al papel del individuo en el cumplimiento de esas expectativas. Las personas a quienes se les asignen responsabilidades en materia de seguridad del software deben poder demostrar que entienden sus responsabilidades y su obligación de rendir cuentas. Las evidencias para respaldar este objetivo podrían incluir descripciones de los puestos de trabajo, acuerdos con los empleados, presentaciones, comunicaciones de la empresa, materiales de formación, correos electrónicos, contenido de la intranet o cualquier otra documentación o registro que ilustre de forma clara y coherente la asignación de las responsabilidades de seguridad, así como el reconocimiento y la comprensión de dichas funciones y responsabilidades.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
1.3 El personal de desarrollo de software tiene habilidades relacionadas con los temas de seguridad de software relevantes para su rol específico, responsabilidad y función de trabajo.	**1.3.a** El evaluador examina las pruebas del proveedor para confirmar lo siguiente: • Se implemente un proceso sólido de gestión y mantenimiento de las habilidades de seguridad del software para el personal de desarrollo de software. • Las habilidades requeridas para cada rol, responsabilidad y función de trabajo están claramente definidas. • Los criterios para mantener las competencias individuales están claramente definidos. • El proceso incluye al menos una revisión anual para garantizar que el personal de desarrollo de software mantenga las habilidades necesarias para llevar a cabo las responsabilidades de seguridad que se le han asignado.	Para ser eficaz en el cumplimiento de sus responsabilidades en materia de seguridad del software, el personal de desarrollo de software debe estar capacitado o tener experiencia en el desempeño de dichas responsabilidades y debe mantener las habilidades apropiadas para llevar a cabo correctamente dichas responsabilidades. Como mínimo, todo el personal de desarrollo de software debe tener una comprensión básica de los conceptos generales de seguridad del software y de las mejores prácticas. Las personas con funciones y responsabilidades especializadas deben poseer, además, conocimientos especializados relacionados con las funciones que desempeñan. Algunos ejemplos de competencias especializadas son el diseño de software seguro (arquitectos de software), las técnicas de codificación segura (desarrolladores de software) y las técnicas de pruebas de seguridad (probadores de software). Los esfuerzos por mantener esas habilidades pueden incluir la formación proporcionada por el proveedor de software, la participación continua en grupos de usuarios locales o regionales, o la obtención y mantenimiento de certificaciones específicas del sector. Corresponde al proveedor de software definir los criterios necesarios para mantener las competencias específicas del puesto de trabajo y confirmar el cumplimiento individual al menos una vez al año. Las evidencias que respalden este objetivo de control pueden incluir políticas y procesos, materiales o contenidos de formación, registros de capacitación que hayan recibido en el puesto de trabajo o asistencia a cursos, certificados de calificación individual, créditos de formación continua o cualquier otra documentación o prueba que demuestre de forma clara y coherente que el personal de desarrollo de software posee y mantiene las habilidades y los conocimientos adecuados para ejercer su función y responsabilidades laborales específicas.
	1.3.b Para obtener una muestra de personal de desarrollo de software, examine las pruebas del proveedor y entreviste al personal para confirmar lo siguiente: • Que los individuos han demostrado que poseen las habilidades requeridas para ejercer su papel, responsabilidad o función de trabajo. • Que los individuos han cumplido con los criterios para mantener sus habilidades individuales.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 2: Política y Estrategia de seguridad de Software El proveedor de software define, mantiene y difunde una política de seguridad del software y una estrategia para garantizar el diseño, desarrollo y gestión seguros de sus productos y servicios. Se supervisa y monitorea el rendimiento con respecto a la estrategia de seguridad de los programas informáticos.		
2.1 Identificación y monitoreo de los requisitos de seguridad y cumplimiento de la normativa del sector aplicables a las operaciones, productos y servicios del proveedor de software y a los datos almacenados, procesados o transmitidos por éste.	**2.1** El evaluador examinará la evidencia suministrada por el vendedor para confirmar lo siguiente: • Que existe un proceso sólido para identificar y supervisar los requisitos de seguridad y cumplimiento de la normativa externa y del sector. • Que el proceso incluye, al menos una vez al año, la revisión de las fuentes de los requisitos de seguridad y cumplimiento en la industria a fin de determinar si e gan generado cambios. • El proceso da como resultado un inventario de los requisitos de seguridad y el cumplimiento de la normativa externa y del sector. • El inventario se actualiza a medida que cambian los requisitos externos de seguridad y de cumplimiento.	Muchas organizaciones están sujetas a requisitos de protección de ciertos tipos de información y datos, tal como la Información Personal Identificable (PII por sus siglas en inglés), los Datos del Titular de la Tarjeta (CHD por sus siglas en inglés) y la Información Sanitaria Protegida (PHI por sus siglas en inglés). Los proveedores de software deben estar al tanto de la evolución de los requisitos industriales y normativos aplicables a sus operaciones y productos. El mantener un conocimiento continuo de las obligaciones externas de seguridad y cumplimiento le permite al proveedor de software garantizar que sus procesos abordan adecuadamente esos requisitos en todo momento, incluso cuando se actualizan o se introduzcan nuevos requisitos. La evidencia para respaldar este objetivo de control podrían incluir políticas y procesos documentados, normas internas, asignaciones de requisitos, presentaciones internas, materiales de formación o cualquier otra documentación o registros que ilustren de forma clara y coherente que el proveedor de software ha realizado los esfuerzos razonables para comprender y supervisar sus requisitos externos de seguridad y cumplimiento.
2.2 Se define una política de seguridad de software y se establecen las normas y objetivos específicos para garantizar que los productos y servicios del proveedor de software se diseñen, desarrollen y mantengan para que sean seguros y resistentes a los ataques de manera que satisfagan las obligaciones de seguridad y	**2.2.a** El evaluador examina la evidencia suministrada por el proveedor para confirmar lo siguiente: • Que existe una política de seguridad del software y se le comunica al personal apropiado del proveedor de software y a los socios comerciales, incluyendo todo el personal de desarrollo de software. • Que como mínimo, la política cubre todos los objetivos de control de esta norma (explícita o implícitamente).	Los proveedores de software deben establecer una política de seguridad del software en toda la empresa para garantizar que todas las personas o equipos, — incluyendo a los socios comerciales pertinentes — que participan en el diseño, el desarrollo y el mantenimiento del software, conozcan y comprendan de forma coherente cómo deben construirse y mantenerse, de forma segura, los productos y servicios de software del proveedor, y cómo deben manejarse los activos críticos. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
cumplimiento del proveedor de software.	• Que la política se define con suficientes detalles como para que las normas y los objetivos de seguridad sean cuantificables. • El equipo directivo del proveedor de software ha aprobado la política de seguridad del software.	La política (o políticas) de seguridad del software debe ser conocida y comprendida a fondo por parte de quienes tienen la responsabilidad de garantizar su cumplimiento, así como por aquellas personas y equipos que pueden afectar la seguridad de los productos y servicios del proveedor de software. El equipo gerencial del proveedor de software debe apoyar abiertamente el establecimiento y la aplicación de la política de seguridad del software a través de las comunicaciones adecuadas al personal del proveedor de software, para reforzar la importancia de la seguridad del software para la organización del proveedor y su liderazgo. Las evidencias que apoyan este objetivo de control pueden incluir políticas y procesos documentados, presentaciones, declaraciones de la misión, correos electrónicos, contenido de la intranet de la empresa u otras comunicaciones formales de la empresa que ilustren de forma clara y coherente los esfuerzos para garantizar que el personal adecuado y los socios comerciales conozcan y comprendan la política de seguridad del software del proveedor.
	2.2.b El evaluador entrevistará una muestra del personal de desarrollo de software para confirmar que conocen y comprenden la política de seguridad del software.	
2.3 Se establece y mantiene una estrategia formal de seguridad del software para garantizar la seguridad de los productos y servicios del proveedor de software y para satisfacer su política de seguridad del software.	**2.3a** El evaluador examinará las evidencias suministradas por el proveedor y entrevistará al personal responsable para confirmar lo siguiente: • El establecimiento de una estrategia para garantizar la seguridad de los productos y servicios del proveedor de software. • Que la estrategia de seguridad del software describa claramente cómo se va a satisfacer la política de seguridad del software. • La estrategia de seguridad del software se basa en las metodologías aceptadas por la industria o se alinea con las mismas. • La estrategia de seguridad del software abarca todo el ciclo de vida de los productos y de los servicios del proveedor de software. • La estrategia de seguridad del software es compartida con el personal adecuado,	Una estrategia de seguridad de software es un plan de alto nivel, una hoja de ruta o una metodología para garantizar el diseño, el desarrollo y el mantenimiento seguro de los productos y servicios del proveedor de software, así como la adhesión a la política de seguridad de software del proveedor. Los proveedores de software deberían adoptar los marcos o metodologías existentes o desarrollar los suyos propios de acuerdo con las prácticas aceptadas por la industria para la gestión segura del ciclo de vida del software. Al alinear su estrategia de seguridad del software con las metodologías aceptadas por la industria, es menos probable que el proveedor de software pase por alto los aspectos importantes de la gestión segura del ciclo de vida del software. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	incluyendo al personal de desarrollo del software. • La estrategia de seguridad de los programas informáticos se revisa al menos una vez al año y se actualiza cuando sea necesario (por ejemplo, cuando evolucionan las necesidades empresariales, los factores externos y los productos y servicios).	Los proveedores de software que desarrollan sus propias metodologías deben entender cómo se diferencian de las metodologías aceptadas por la industria, identificar cualquier vacío y garantizar que se mantienen las pruebas suficientes para ilustrar claramente de qué forma sus metodologías son al menos tan eficaces como las aceptadas por la industria. Entre los ejemplos de las metodologías aceptadas por la industria que se utilizan habitualmente como puntos de referencia para el desarrollo y la gestión de software seguro se encuentran, entre otros, las versiones actuales de: • *ISO/IEC 27034 Directrices de Seguridad de la Aplicación.* • *Construcción de la Seguridad en el Modelo de Madurez (BSIMM* por sus siglas en inglés) • *OWASP Modelo de Madurez de la Garantía del Software (Abierto) (SAMM por sus siglas en inglés)* • *Publicación Especial NIST 800-160 y sus anexos*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	2.3.b El asesor entrevistará una muestra del personal de desarrollo de software para confirmar que conocen y comprenden la política de seguridad del software.	La estrategia de seguridad del software debe evolucionar a medida que lo hacen los factores internos, como la estrategia empresarial del proveedor de software o las ofertas de productos y servicios, o los factores externos, como los requisitos externos de seguridad y cumplimiento. Por lo tanto, la estrategia de seguridad del software no es estática y debe ser revisada y actualizada periódicamente para mantener su alineación con las necesidades y prioridades del negocio. Las evidencias para respaldar este requisito podrían incluir planes o metodologías de seguridad documentados, presentaciones, políticas y procesos, materiales de formación, actas de reuniones, notas de los entrevistadores, correos electrónicos o comunicaciones ejecutivas, mapas o referencias de las metodologías aceptadas por el sector, resultados de análisis de deficiencias o cualquier otro registro o documentación que ilustre de forma clara y coherente que el proveedor ha realizado un esfuerzo razonable para desarrollar y mantener actualizada una estrategia formal para satisfacer la política de seguridad del software del proveedor.
2.4 Los procesos de garantía de la seguridad del software se aplican y mantienen a lo largo de todo el ciclo de vida del software. ***Nota:*** *Este objetivo de control se centra en la gestión global de los procesos de garantía de seguridad y proporciona la base para los procesos de garantía específicos definidos en este documento.*	**2.4a** El evaluador examinará las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que los procesos de garantía de la seguridad del software se definen, aplican y mantienen. • Que se mantiene un inventario de los procesos de garantía de seguridad del software.	Que los procesos de garantía de seguridad del software son actividades que se implementan para llevar a cabo la estrategia de seguridad del software del proveedor y para facilitar el diseño, el desarrollo y el mantenimiento seguro del mismo. A fin de garantizar que se cumplan los requisitos de seguridad y de conformidad, que se satisfaga la política de seguridad del software y que los productos y los servicios del proveedor de software sean seguros y resistentes a los ataques, los proveedores de software deben definir dichos procesos a lo largo de todas las fases del ciclo de vida del software. Pueden incluir los "puntos de control" de la seguridad, que son puntos distintos dentro del proceso de desarrollo del software en los cuales éste se comprueba para asegurarse de que se est{a cumpliendo con los requisitos de seguridad. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
		Algunos ejemplos de los procesos y controles de garantía de la seguridad del software son las revisiones del diseño del software, las revisiones automatizadas del código, las pruebas funcionales específicas de seguridad y los procesos de gestión de cambios. Para las organizaciones que aprovechan las metodologías ágiles de desarrollo de software, los puntos de control de seguridad pueden incorporarse a los criterios de aceptación de la "historia" o a los criterios para determinar cuándo se considera que el trabajo se ha “hecho”.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	2.4.b Para obtener una muestra del proceso de garantía de seguridad del software, el evaluador deberá examinar la evidencia suministrada por el proveedor y entrevistar al personal para confirmar lo siguiente: • Que los procesos de garantía de seguridad del software abordan claramente las normas y los objetivos específicos de la política de seguridad del software del proveedor. • Que los procesos de garantía de seguridad del software están alineados con la estrategia de seguridad del software del proveedor. • Que al personal del proveedor de software, incluyendo al personal de desarrollo de software, se le asigna la responsabilidad y la obligación de rendir cuentas en lo relacionado con la ejecución y el desempeño en el proceso de garantía de seguridad de acuerdo con el objetivo de control 1.2. • Que los individuos o equipos responsables de realizar y mantener cada proceso de garantía de seguridad son claramente conscientes de sus responsabilidades. • Que los resultados de cada proceso de garantía de seguridad se supervisan de acuerdo con el objetivo de control 2.6.	Las evidencias para respaldar este requisito pueden incluir políticas y procesos documentados, inventarios de controles de seguridad, resultados de las herramientas de Gestión, Riesgo y Cumplimiento (GRC por sus siglas en inglés) u otras herramientas de gestión, documentación de requisitos específicos del software, o cualquier otra prueba que identifique de forma clara y coherente los procesos de garantía de la seguridad del software que se han implementado e ilustre que los procesos de garantía de la seguridad son adecuados para la función que pretenden proporcionar. Adicionalmente, las evidencias para ilustrar que los procesos de garantía de la seguridad del software se aplican correctamente pueden incluir resultados del sistema o del proceso, como modelos de amenazas, resultados de pruebas de seguridad, datos de seguimiento de errores, datos de registro de auditoría, respuesta a incidentes, etc.
2.5 Las evidencias se generan y se mantienen para demostrar la eficacia de los procesos que garantizan la seguridad del software.	**2.5.a** El evaluador examinará las evidencias suministradas por el proveedor, incluyendo el inventario de procesos de garantía de seguridad del software descrito en el requisito de la prueba 2.4.a , y entrevistará al personal para confirmar que se generan y mantienen las evidencias para todos los procesos que garantizan la seguridad.	Para demostrar la eficacia de los procesos que garantizan la seguridad del software, se deben generar y mantener evidencias de cada proceso a fin de demostrar que llevan a resultados directos o que contribuyen con los resultados de seguridad esperados, por ejemplo, menos vulnerabilidades o mayor resistencia ante los ataques. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
		Las evidencias deben recopilarse con frecuencia y mantenerse actualizadas para garantizar que reflejen con exactitud la eficacia continua de los procesos de garantía de la seguridad. Sin un historial del desempeño de los procesos de garantía de la seguridad del software, resulta casi imposible realizar un análisis eficaz de la causa primaria cuando dichos procesos no producen los resultados esperados.
	2.5.b Para obtener una muestra de procesos que garanticen la seguridad, el evaluador examinará las evidencias y los demás resultados de los procesos y entrevistará al personal para confirmar que las evidencias generadas para cada proceso demuestran razonablemente que el proceso funciona de forma eficaz y según lo previsto.	Las evidencias para apoyar este objetivo podrían incluir los inventarios de control de seguridad y generación de pruebas, informes de vulnerabilidad, resultados de pruebas de penetración o cualquier otro registro y una prueba que ilustre de forma clara y coherente que se generan evidencias para todos los procesos que garantizan la seguridad del software y que las evidencias ilustran claramente la eficacia de los procesos.
2.6 Se detectan fallos o debilidades en los procesos que pretenden garantizar la seguridad del software. Los procesos que pretenden garantizar la seguridad que son débiles o ineficaces se actualizan, aumentan o sustituyen.	**2.6a** El evaluador examinará las suministradas por el proveedor para confirmar lo siguiente: • Que exista un proceso sólido para detectar y evaluar los procesos que son débiles o ineficaces utilizados para garantizar la seguridad. • Que se definan y justifiquen los criterios para determinar que un proceso que pretende garantizar la seguridad es débil o ineficaz. • Que los procesos que pretenden garantizar la seguridad se actualicen, aumenten o sustituyan cuando se consideren débiles o ineficaces.	Que los proveedores de software deben supervisar sus procesos de garantía de seguridad para confirmar que continúan siendo apropiados (es decir, que son aptos para el propósito) y que son eficaces para el propósito y función previstos. Por ejemplo, el uso de las revisiones manuales del código puede ser suficiente para detectar todos los errores de codificación y las vulnerabilidades del software que tienen una base de código muy limitada. Sin embargo, a medida que la base del código crece, el uso de las revisiones manuales del código para el mismo propósito se hace cada vez menos práctico o insuficiente, y se deben utilizar herramientas de pruebas automatizadas (como escáneres de código estático automatizados y herramientas de análisis de software dinámico). Un método para detectar los controles de seguridad que son débiles o ineficaces consiste en definir un conjunto de métricas o tendencias que puedan utilizarse para medir la eficacia de los procesos que garantizan la seguridad. Por ejemplo, los resultados de las pruebas de seguridad de un proveedor pueden proporcionar una mayor comprensión de la eficacia de los procesos que garantizan la seguridad. *(continúa en la siguiente página)*
	2.6.b Para obtener una muestra de los procesos que garantizan la seguridad identificados en el Objetivo de Control 2.4 , el evaluador entrevistará al personal y examinará cualquier evidencia adicional necesaria para determinar si se produjeron fallos o debilidades en dichos procesos de seguridad, y para confirmar que los procesos que sean débiles o	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	ineficaces hayan sido actualizados, aumentados o sustituidos.	Si las pruebas de seguridad encuentran repetidamente vulnerabilidades en el software, esto puede ser un indicativo de que los procesos que pretenden garantizar la seguridad aplicables no se están ejecutando correctamente o no están funcionando como se pretende. Otro método para detectar los procesos que pretenden garantizar la seguridad y que son débiles o ineficaces sería realizar revisiones periódicas de dichos procesos y de las evidencias generadas por los mismos para verificar que siguen siendo apropiados para su propósito. Las evidencias para respaldar este requisito pueden incluir evidencias generadas por el proceso, resultados de pruebas de seguridad, análisis de la causa primaria, acciones de corrección documentadas o cualquier otra evidencia que ilustre de forma clara y coherente que la eficacia de los procesos que garantizan la seguridad del software se supervisa, que se detectan los fallos y las debilidades y que los procesos que pretenden garantizar la seguridad se actualizan, aumentan o sustituyen cuando dejan de ser eficaces para satisfacer su objetivo.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Ingeniería de Software Seguro

El software se diseña y desarrolla para proteger los activos de software críticos y para que sea resistente a los ataques.

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 3: Identificación y Mitigación de amenazas El proveedor de software identifica, evalúa y gestiona continuamente los riesgos de su software y de sus servicios.		
3.1 Se identifican y clasifican los activos críticos.	**3.1** El evaluador examinará las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que existe un proceso sólido para identificar y clasificar los activos críticos. • Que se definan los criterios para identificar los activos críticos y determinar los requisitos de confidencialidad, integridad y resiliencia de todos los activos críticos. • Que el proceso abarca todos los tipos de activos críticos, incluyendo los datos, recursos y funciones confidenciales, para el software del proveedor. • El proceso da como resultado un inventario de los activos críticos utilizados por el software del proveedor.	Antes de que el proveedor de software pueda determinar cómo asegurar y defender eficazmente su software contra los ataques, primero debe desarrollar un conocimiento profundo de los activos críticos del software que podrían ser el objetivo de los atacantes. Los activos críticos incluyen cualquier data confidencial que haya sido recolectada, procesada o transmitida por el software del proveedor, así como cualquier otra función y recursos confidenciales dentro del software o que sea utilizado por éste. Algunos ejemplos de las técnicas de análisis que podrían utilizarse para identificar los activos críticos son, entre otros, el Análisis del Impacto de la Misión (MIA por sus siglas en inglés), el Análisis de la Red de Dependencia Funcional (FDNA por sus siglas en inglés) y el Análisis de la Amenaza de la Misión.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
3.2 Las amenazas al software y los puntos débiles de su diseño se identifican y evalúan continuamente.	**3.2.a** El evaluador examinará las evidencias suministradas por el proveedor, incluyendo la documentación del proceso y los resultados de la evaluación, para confirmar lo siguiente: • Que existe un proceso sólido para identificar, evaluar y supervisar las amenazas del software y las debilidades del diseño (es decir, los defectos). • Que la evaluación toma en cuenta todas las entradas y las salidas del software, los flujos de los procesos o datos, los límites de confianza y los puntos de decisión, y cómo estos pueden ser explotados por un atacante. • Que la evaluación toma en cuenta la totalidad de la base del código, incluyendo el uso de componentes o bibliotecas de terceros, de código abierto o compartidos, APIs, servicios y aplicaciones utilizadas para la entrega y el funcionamiento del software que pueden ser aprovechados cuando haya un ataque. • La evaluación da como resultado un inventario registrado de amenazas y defectos de diseño. • Las evaluaciones se realizan de forma rutinaria para tener en cuenta los cambios en las amenazas existentes o la aparición de nuevas amenazas o defectos de diseño.	El determinar cómo asegurar y defender eficazmente el software contra los ataques requiere de un conocimiento profundo de las amenazas y vulnerabilidades específicas aplicables al software del proveedor. Esto suele implicar la comprensión de lo siguiente: • Las motivaciones que puede tener un atacante para atacar el software; • Las debilidades en el diseño del software que un atacante podría intentar explotar; • La posibilidad de explotar los puntos débiles identificados; y • El impacto de un ataque exitoso. Esta información ayuda al proveedor de software a identificar las amenazas y los defectos de diseño que presentan el riesgo más significativo e inmediato, y a priorizar las actividades de corrección necesarias para hacerles frente. La información relacionada con las amenazas de software puede obtenerse a partir de diversas fuentes, tanto externas como internas. Algunos ejemplos de fuentes externas son las publicaciones de organizaciones tales como SANS, MITRE y CERT, las cuales se especializan en el seguimiento de las vulnerabilidades de los sistemas y las técnicas de ataque más comunes, o las fuentes específicas de la industria que proporcionan información sobre las amenazas para sectores concretos, como FS-ISAC para la industria de los servicios financieros y R-CISC para la industria minorista. Otras fuentes externas de información sobre las amenazas y debilidades de diseño podrían ser los proveedores de tecnología, las comunidades de usuarios de código abierto, las publicaciones de la industria y los trabajos académicos. Las fuentes internas podrían incluir informes de los equipos internos de investigación y diseño, modelos formales de amenazas o datos de actividad real de los equipos internos de seguridad u operaciones. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	3.2.b Cuando se utilicen componentes de software de código abierto como parte del software, el evaluador examinará las pruebas del proveedor, incluyendo la documentación del proceso y los resultados de la evaluación, para confirmar que estos componentes se gestionan de la siguiente manera: • Se mantiene un inventario de los componentes de código abierto utilizados en el software del proveedor. • Existe un proceso sólido para analizar y mitigar el uso de componentes de código abierto que tienen vulnerabilidades conocidas. • El proveedor de software supervisa las vulnerabilidades de los componentes de código abierto durante todo su uso o inclusión en el software del proveedor. • Se define una estrategia de parcheo adecuada para los componentes de código abierto.	Cuando se utilicen componentes de software de código abierto, el proveedor de software debe tener en cuenta los riesgos asociados al uso de los componentes de código abierto y la medida en que el proveedor de software de código abierto gestiona la seguridad de dichos componentes. Además, el proveedor de software tendrá que confirmar que dispone de un soporte, incluyendo los parches de seguridad actualizados, (ya sea proporcionado por una entidad interna o externa) para el componente de código abierto. El uso de componentes de código abierto debe estar respaldado por una política clara acerca de cómo se evalúan e implementan esos componentes. Debe existir un sistema de apoyo confiable para identificar los errores o problemas y evaluarlos y solucionarlos a tiempo. Cuando se identifiquen vulnerabilidades en los componentes de código abierto que sean aplicables a su software, los proveedores de software deben contar con los procesos para analizar dichas vulnerabilidades y actualizar los componentes a versiones adecuadas y no vulnerables de manera oportuna. Cuando los parches para los componentes de código abierto ya no están disponibles, esos componentes deben sustituirse por otros que tengan un soporte activo. Los proveedores deben identificar y establecer fuentes y procesos para gestionar las vulnerabilidades de los componentes de código abierto que sean apropiados para su diseño de software y su frecuencia de publicación.
	3.2.c Para obtener una muestra de software del proveedor, el evaluador examinará los resultados de la evaluación del software seleccionado para confirmar lo siguiente: • Que durante la evaluación se tomaron en cuenta todas las entradas y salidas del software, los flujos de procesos o datos, los límites de confianza y los puntos de decisión. • La totalidad de la base del código, incluyendo la forma en que se ha tomado en cuenta durante la evaluación, el uso de los componentes o de las bibliotecas de terceros de código abierto o compartido, API, servicios y aplicaciones utilizados para la entrega y el funcionamiento del software.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
3.3 Los controles de seguridad del software se implementan en el software para mitigar las amenazas y los puntos débiles del diseño.	**3.3.a** El evaluador examinará las evidencias suministradas por el proveedor, incluyendo la documentación del proceso y de la información sobre amenazas y diseño específicos del software, para confirmar lo siguiente: • Que existe un proceso sólido para definir los requisitos de seguridad específicos del software e implementar controles de seguridad en el software para mitigar las amenazas y los defectos de diseño del mismo. • Que las decisiones sobre la conveniencia y el modo de mitigar una amenaza específica o un defecto de diseño se registran, justifican y aprueban por parte del personal adecuado. • Que cualquier riesgo residual restante se registra, se justifica y es aprobado por parte del personal adecuado.	Para garantizar que su software es resistente a los ataques, los proveedores de software deben implementar controles o contra medidas específicas en su software para mitigar las amenazas específicas y las debilidades de diseño. Algunos ejemplos de estos controles son el uso de mecanismos de autenticación de múltiples factores para evitar que personas no autorizadas accedan a los activos críticos, y a los mecanismos de registro para detectar si los mecanismos de autenticación se han eludido y cuándo. Otros ejemplos son el uso de rutinas de validación de entradas o consultas parametrizadas para proteger el software de los ataques de inyección SQL. Salvo en los casos en los cuales se definan los controles y las contra medidas de seguridad del software específicos dentro de esta norma, corresponde al proveedor determinar los controles de seguridad del software más adecuados para que se apliquen. Los controles específicos utilizados dependerán de las amenazas del software identificadas en el Objetivo de Control 3.2, así como de la arquitectura del software, la función prevista del software, los datos que maneja y los recursos externos que utiliza. Las evidencias para respaldar este objetivo de control pueden incluir la documentación de los requisitos específicos del software, listas de características, los inventarios de los controles de seguridad, la documentación de la gestión de cambios, los informes de evaluación de riesgos, los resultados de las pruebas o cualquier otra prueba o información que ilustre de forma clara y coherente que el proveedor de software implementa y mantiene controles de seguridad para que el software aborde los riesgos de dicho software.
	3.3.b El evaluador examinará las pruebas y entrevistará al personal para confirmar lo siguiente: • Que las decisiones acerca de si hay que mitigar una amenaza específica o un defecto de diseño y cómo hacerlo son razonablemente justificadas. • Cualquier riesgo residual restante sea razonablemente justificado.	
	3.3.c El evaluador examinará las evidencias suministradas por el proveedor para confirmar que se han implementado los controles de seguridad para mitigar todas las amenazas y defectos de diseño identificados.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
3.4 Se detectan fallos o debilidades en los controles de seguridad del software. Los controles de seguridad débiles o ineficaces se actualizan, aumentan o sustituyen.	**3.4.a** El evaluador examinará las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que existe un proceso sólido para identificar controles de seguridad de software débiles o ineficientes y actualizar, aumentar o reemplazarlos. • Se definen y justifican los criterios para determinar si un control de seguridad es débil o ineficaz. • El proceso implica la supervisión de la efectividad del control de seguridad a lo largo del ciclo de vida del software. • Los controles de seguridad débiles o ineficaces se actualizan, aumentan o sustituyen oportunamente cuando se detectan.	Los proveedores deben supervisar y / o probar rutinariamente su software para confirmar que los controles de seguridad del software implementados siguen siendo apropiados (es decir, adecuados para el propósito) y eficaces para mitigar suficientemente los riesgos que se encuentran en evolución o los defectos de diseño. Por ejemplo, un requisito de seguridad específico del software puede exigir el uso de la criptografía para proteger las comunicaciones del software. Aunque el uso de SSL puede haber sido suficiente para el diseño y el lanzamiento inicial del software, SSL ya no es suficiente para proteger adecuadamente las comunicaciones, ya que las nuevas amenazas y métodos de ataque han reducido significativamente su efectividad para controlar la seguridad. Por lo tanto, es imperativo que los proveedores cuenten con procesos para supervisar continuamente los controles de seguridad implementados para asegurarse de que siguen siendo adecuados y suficientes para mitigar las amenazas que se encuentran en evolución y los defectos de diseño durante toda la vida útil del software. Las evidencias para respaldar este requisito pueden ser la documentación específica del software, las listas de características, los inventarios de los controles de seguridad específicos del software, la documentación de gestión de cambios, los informes de evaluación de riesgos, los resultados de las pruebas de penetración, los resultados de los sistemas de supervisión activos, los datos del programa de recompensas por errores o cualquier otra prueba o información que ilustre de forma clara y coherente que la efectividad de los controles de seguridad del software está siendo supervisada y que los controles de seguridad específicos del software se actualizan, aumentan o sustituyen cuando dejan de ser eficientes para satisfacer su objetivo de resistir ante los ataques.
	3.4.b El evaluador examinará la evidencia suministrada por el proveedor, incluyendo los datos específicos del software o los resultados de las pruebas, y los detalles de las actualizaciones específicas del software para confirmar lo siguiente: • Que los controles de seguridad que se han considerado "débiles" o "ineficaces" se han actualizado, aumentado o sustituido. • Que las decisiones sobre la sustitución y el aumento para controlar la seguridad que son débiles o ineficaces se toman de acuerdo con los criterios definidos y con el objetivo de control 3.3.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 4: Detección y Mitigación de las Vulnerabilidades El proveedor de software detecta y mitiga las vulnerabilidades del software para garantizar que su software siga siendo resistente ante los ataques durante todo su ciclo de vida.		
4.1 Las vulnerabilidades del software existentes y emergentes se detectan a tiempo.	**4.1.a** El evaluador examina las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que exista un proceso sólido para poner a prueba los programas informáticos a fin de detectar la existencia y la aparición de vulnerabilidades (es decir, pruebas de seguridad). • Las herramientas o métodos utilizados para las pruebas de seguridad son apropiados para detectar las vulnerabilidades aplicables al software del proveedor, y son adecuados para las arquitecturas del software, y los lenguajes y marcos de desarrollo del software utilizados. • Las pruebas de seguridad se realizan a lo largo de todo el ciclo de vida del software, incluso después de su publicación. • Las pruebas de seguridad tienen en cuenta la totalidad de la base de código, incluyendo la detección de vulnerabilidades en cualquier componente y biblioteca de terceros, de código abierto y compartido. • Las pruebas de seguridad las realiza el personal autorizado y el proveedor objetivo o terceros. • Las pruebas de seguridad dan como resultado un inventario de las vulnerabilidades identificadas. • Se registran y conservan los detalles de las pruebas de seguridad, incluyendo las herramientas utilizadas, sus configuraciones y las pruebas específicas realizadas.	El software debe supervisarse o probarse de forma rutinaria para confirmar que las vulnerabilidades se identifican y mitigan antes de que el software o las actualizaciones del código se liberen en la producción, y para abordar cualquier vulnerabilidad que se pueda haber descubierto desde la liberación. Las pruebas de seguridad rutinarias deben realizarse antes o como parte del proceso de envío del código para detectar los errores de codificación o el uso de funciones inseguras. También podrían realizarse durante las pruebas unitarias, de integración, de regresión o de pruebas de ínter-operabilidad, o durante las pruebas de seguridad independientes. Las pruebas de seguridad deben realizarse de forma coherente y a lo largo de todas las etapas del ciclo de vida del software, incluso durante las distintas fases previas a la publicación del proceso de desarrollo del software y después de la publicación del código, para garantizar que el software está libre de vulnerabilidades en el momento de su lanzamiento y en cualquier actualización posterior, y que permanece libre de vulnerabilidades durante toda su vida útil. Las pruebas de seguridad deben realizarse por el personal del proveedor o terceros debidamente capacitados. Además, el personal encargado de las pruebas de seguridad debe poder realizarlas de forma objetiva y estar autorizado para comunicar cualquier vulnerabilidad identificada al personal de gestión o de desarrollo adecuado para que pueda tratarse adecuadamente. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	4.1.b El evaluador examinará las pruebas, incluyendo las configuraciones de las pruebas de seguridad específicas del software y los resultados de las pruebas para confirmar lo siguiente: • Que las herramientas de las pruebas de seguridad están configuradas de forma adecuada para las pruebas que se pretenden realizar. • Las pruebas de seguridad tienen en cuenta la totalidad de la base de código, incluyendo la detección de vulnerabilidades en cualquier componente y biblioteca de terceros, de código abierto y compartido. • Las pruebas de seguridad las realiza y autoriza el personal autorizado y el proveedor objetivo o los terceros.	Las evidencias para respaldar este objetivo de control podrían incluir la documentación de los requisitos específicos del software, los resultados de las pruebas de seguridad, las listas de las características, la documentación de la gestión de cambios, las entradas en la base de datos del flujo de trabajo del proveedor (seguimiento de errores) o cualquier otra prueba o información que demuestre de forma clara y coherente que las pruebas de seguridad se realizan de forma rutinaria para detectar las vulnerabilidades que tiene el código antes de su lanzamiento, así como las vulnerabilidades descubiertas después del lanzamiento del código.
	4.1.c El evaluador examinará las pruebas del proveedor y entrevistará al personal para confirmar que el personal responsable de las pruebas tiene conocimientos y habilidades en las siguientes áreas de acuerdo con el objetivo de control 1.3: • Técnicas de Pruebas de Seguridad del Software • Ajustes, configuraciones y uso recomendado de las herramientas de las pruebas de seguridad	
	4.1.d Para obtener una muestra de software de parte del proveedor, examine los resultados de las pruebas específicas del software para confirmar que las pruebas de seguridad se realizan durante todo el ciclo de vida del software.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
4.2 Las vulnerabilidades recién descubiertas se solucionan a tiempo. Se evita re-introducir vulnerabilidades similares o previamente resueltas.	**4.2.a** El evaluador examina la evidencia suministrada por el proveedor para confirmar lo siguiente: • Existe un proceso sólido para distribuir y desplegar las correcciones de las vulnerabilidades recién descubiertas y evitar re-introducir las vulnerabilidades previamente resueltas. • El proceso incluye métodos para evitar que se re-introduzcan en el software las vulnerabilidades previamente resueltas u otras similares. • Se definen y justifican los criterios para determinar la "criticidad" o "gravedad" de las vulnerabilidades y la forma de abordarlas. • Las correcciones para abordar las vulnerabilidades en el código de producción están disponibles y se despliegan de acuerdo con los criterios definidos. • Las decisiones de no proporcionar los arreglos de acuerdo con los criterios definidos son aprobadas y justificadas por el personal apropiado en cada caso por separado.	Las vulnerabilidades deben abordarse de forma proporcional al riesgo que suponen para el software o para las partes interesadas. Las vulnerabilidades más críticas o graves, —es decir, las que tienen una mayor posibilidad de ser explotadas y / o un mayor impacto para las partes interesadas—, se deben parchear inmediatamente, seguidas de las que tienen una posibilidad de ser explotadas y / o un impacto de moderado a bajo. Además, el descubrimiento de nuevas clases de vulnerabilidades se debe utilizar como fuente de información para mejorar el proceso. El software debe revisarse para detectar los casos de vulnerabilidades similares, y los procesos de desarrollo del proveedor se deben actualizar para permitir la detección y mitigación de dichas vulnerabilidades en el futuro. En algunos casos, puede resultar poco práctico para el proveedor corregir todas las vulnerabilidades identificadas antes de la publicación del código de producción o de las actualizaciones. En tales circunstancias, el proveedor debe tener una metodología con criterios claramente definidos para priorizar las correcciones de la vulnerabilidad. El resultado predeterminado siempre debería ser que las vulnerabilidades se solucionen antes de que se publique el software. En aquellos casos en los cuales no es posible solucionar una vulnerabilidad antes de su publicación, deberá invocarse un proceso de excepción en el cual participe la gerencia a un nivel acorde con la gravedad de la vulnerabilidad. El proceso debe incluir una justificación documentada de por qué no se proporcionó una solución para abordar la vulnerabilidad. Si no es posible mitigar una determinada vulnerabilidad antes de su publicación, el proveedor debe proporcionarles a las partes interesadas, la orientación adicional para mitigar el riesgo de explotación hasta que se pueda disponer de una actualización de seguridad que corrija la vulnerabilidad. *(continúa en la siguiente página)*
	4.2.b Para obtener una muestra del software del proveedor, el evaluador examinará los resultados de las pruebas de seguridad específicas del software y los detalles de las actualizaciones del software para confirmar que las correcciones de seguridad se ponen a disposición y se despliegan (cuando corresponda) de acuerdo con los criterios definidos.	
	4.2.c Para obtener una muestra del software del proveedor, el evaluador entrevistará al personal para confirmar que las decisiones de no proporcionar las correcciones de seguridad de	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	acuerdo con los criterios definidos están justificadas por parte del personal adecuado.	Bajo ninguna circunstancia se debe re-introducir, en el código de producción, una vulnerabilidad previamente resuelta, ni se deben re-introducir vulnerabilidades similares dentro de la misma clase de vulnerabilidades. Deben aplicarse los procesos de garantía y salvaguardas adicionales para garantizar el evitar estos incidentes. Los procesos específicos para evitar estos sucesos dependerán en gran medida de cómo esté estructurado el software del proveedor y de cómo éste gestione las actualizaciones del mismo. Corresponde al proveedor de software determinar los métodos más adecuados para evitar la re-introducción de vulnerabilidades en el código de producción.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Software Seguro y Gestión de Dato

La confidencialidad e integridad del software y sus activos críticos se mantienen durante todo el ciclo de vida del software.

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 5: Gestión del Cambio El proveedor de software identifica y gestiona todos los cambios del software a lo largo de su ciclo de vida.		
5.1 Todos los cambios en el software se identifican, evalúan y aprueban.	**5.1.a** El evaluador examinará las pruebas del proveedor y entrevistará al personal para confirmarlo: • Existe un proceso sólido para identificar, evaluar y aprobar todos los cambios del software. • El proceso incluye un análisis del impacto respecto a la seguridad de todos los cambios. • El proceso da como resultado un inventario de todos los cambios realizados en el software, incluyendo un registro del impacto determinado en la seguridad. • Se registran todas las decisiones de gestión del cambio. • Todos los cambios implementados los autoriza el personal responsable. • El inventario de los cambios identifica al creador individual del código y a la persona que autoriza el cambio, para cada cambio del código. • Todas las decisiones de aplicar los cambios están justificadas.	Todos los cambios en el software deben definirse, documentarse, aprobarse y rastrearse para que cualquier vulnerabilidad atribuida a dichos cambios se pueda identificar y resolver lo antes posible. Cuanto más difícil sea rastrear las vulnerabilidades hasta los cambios que las introdujeron, más tiempo se tarda en resolverlas,— lo cual hace que el software corra un mayor riesgo de ser atacado o puesto en peligro. Es imperativo comprender el riesgo de seguridad que implica un cambio en el software para asegurarse de que se aborda correctamente. Suele implicar la comprensión de los tipos de funcionalidad del software a los cuales afecta el cambio (por ejemplo, la funcionalidad que trata procesos de encriptación o autenticación), el tipo de activos de información a los cuales la funcionalidad puede acceder o manipular, la probabilidad de explotación de la vulnerabilidad de manera exitosa y el impacto que un ataque exitoso puede tener para las partes interesadas.
	5.1.b Para obtener una muestra de los cambios, el evaluador examinará la documentación o las pruebas específicas del software y de los cambios para confirmar lo siguiente: • Que todos los cambios los autoriza el personal responsable.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	• Que todas las decisiones de aplicar los cambios se registran e incluyen la justificación del cambio. • Que el inventario de los cambios identifica claramente al creador individual del código y a la persona que autoriza el cambio, para todos los cambios de código.	
5.2 Todas las versiones del software se identifican de forma única y se rastrean a lo largo del ciclo de vida del software.	**5.2.a** El evaluador examina las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que se define un sistema o metodología formal para identificar de forma única cada versión del software. • Que el sistema o metodología incluye la disposición de los identificadores únicos o de los elementos de la versión de forma secuencial y lógica. • Que todos los cambios en la funcionalidad del software están claramente asociados a una única versión del mismo.	Sin una metodología de una versión bien definida, es posible que los cambios en el software no se identifiquen correctamente y que los clientes y los integradores y revendedores no entiendan el impacto de dichos cambios. *(continúa en la siguiente página)*

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
	5.2.b Para obtener una muestra de actualizaciones del software, el evaluador examinará la evidencia suministrada por el proveedor, incluyendo la documentación específica de cambios, para confirmar lo siguiente: • Que las versiones de los programas informáticos se actualizan de acuerdo con el sistema o la metodología de las versiones definidas. • Que todos los cambios en la funcionalidad del software están claramente asociados a una única versión del mismo.	El sistema o la metodología adoptada por el proveedor debe permitir el distinguir fácilmente las diferentes versiones de un producto del software. Para garantizar que una versión del software representa con exactitud la versión de lanzamiento, el sistema o metodología de la versión debe integrarse a las funciones aplicables del ciclo de vida, tal como el control del código y la gestión de cambios. El sistema o metodología de la versión debe abarcar todos los cambios de todos los componentes relevantes del software. Dado que pueden producirse varias iteraciones de un componente del software para una sola versión del software, el sistema o metodología de la versión debe identificar fácilmente la versión de cada componente asociada a una versión del software específica. El método utilizado para identificar las versiones del software, por ejemplo, un esquema de numeración de las versiones, debe documentarse y reflejar el tipo de cambio y su impacto en el software. Para software destinados a ser validados en el Marco de Seguridad del Software de PCI, el sistema o metodología de la versión del proveedor es importante para determinar las actualizaciones de la Lista de Software Pago Validado por PCI SSC. Consulte la *Guía del Programa de SLC Seguro de PCI* para información adicional.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 6: Protección de la Integridad del Software La integridad del software está protegida durante todo el ciclo de vida del mismo.		
6.1 Todo el código del software, incluyendo los componentes de terceros, se mantiene durante todo el ciclo de vida del software.	**6.1** El evaluador examinará las pruebas, entrevistará al personal y observará las herramientas y los procesos para confirmar lo siguiente: • Que existe un proceso, mecanismo y / o herramienta o herramientas robustas para proteger la integridad del código del software, incluyendo los componentes de terceros. • Los procesos, mecanismos y / o herramientas son razonables y adecuados para proteger la integridad del código del software. • Los procesos, mecanismos o el uso de herramientas permiten detectar a tiempo cualquier intento no autorizado de manipulación o acceso al código del software. • Los intentos no autorizados de manipular o acceder al código del software se investigan oportunamente.	Las prácticas efectivas de control del código del software ayudan a garantizar que todos los cambios en el código estén autorizados y los realicen sólo quienes tienen una razón legítima para cambiar el código. Ejemplos de estas prácticas son los procedimientos de entrada y salida del código que tienen controles estrictos de acceso, y una comparación, por ejemplo, utilizando una lista de verificación, inmediatamente antes de actualizar el código para confirmar que no se ha modificado la última versión aprobada. Es importante que los controles abarquen todo el código del software, los componentes y las bibliotecas de terceros, los archivos de configuración, etc., que el proveedor controla. Es necesario mantener la integridad y la confidencialidad de estos activos, ya que a menudo contienen datos sensibles tales como la propiedad intelectual, por ejemplo, la lógica empresarial de las funciones de seguridad, la configuración de las funciones criptográficas (por ejemplo, la criptografía de la caja blanca), etc.
6.2 Los lanzamientos y las actualizaciones de software se entregan de una manera segura que garantiza la integridad del código actualizado.	**6.2** El evaluador examinará las pruebas del proveedor, entrevistará al personal y observará las herramientas y los procesos para confirmar lo siguiente: • Que existe un proceso, mecanismo y / o herramienta o herramientas maduras para garantizar la integridad de las actualizaciones del software durante la entrega. • Que los procesos, mecanismos y / o herramientas son razonables y adecuados para proteger el código de actualización. • Que los procesos, mecanismos y / o el uso de herramientas dan como resultado la entrega segura del código actualizado.	Que las actualizaciones de seguridad deben incluir un mecanismo dentro del proceso de actualización para verificar que el código actualizado no se ha sustituido ni manipulado. Algunos ejemplos de comprobaciones de integridad son las sumas de comprobación y los certificados firmados digitalmente de forma correcta. Para garantizar que los controles implementados sean adecuados para hacer frente a los vectores de ataque en evolución, los proveedores de software deben realizar revisiones periódicas para confirmar su continua efectividad.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 7: Protección de Datos Confidenciales La confidencialidad de datos de producción confidencial se mantiene en los sistemas del proveedor.		
7.1 Los datos de producción confidenciales sólo se recogen y conservan en los sistemas de los proveedores de software cuando existe una necesidad comercial o técnica legítima.	**7.1.** El evaluador examinará las evidencias suministradas por el proveedor para confirmar lo siguiente: • Que existe un proceso sólido para registrar y autorizar la recolección y retención de cualquier información confidencial. • Que se mantiene un inventario de la producción de información confidencial capturada o almacenada por los productos y los servicios del proveedor de software. • Que las decisiones para utilizar información confidencial sea aprobada por personal apropiado del proveedor de software. • Que las decisiones de utilizar la información confidencial sea registrada de manera razonable y justificable.	A fin de proteger la confidencialidad de la cualquier información sensitiva, es decir, información que pertenece a cualquier entidad que no sea el proveedor del software - y que sea almacenada en sistemas del proveedor de software, dichos datos no deben utilizarse nunca con fines distintos de aquellos para los que se recogieron originalmente. Si el proveedor de software presta sus servicios a las partes interesadas, lo cual podría dar lugar a la recopilación de datos confidenciales —por ejemplo, para la resolución de problemas o la depuración—, el proveedor de software debe registrar qué elementos de los datos específicos recopila y conserva, y comunicar claramente a sus clientes y a las demás partes interesadas pertinentes, qué elementos de los datos se recopilan y por qué se recopilan. El inventario de información confidencial retenida por el proveedor de software debe incluir la identificación de los elementos de datos específicos capturados, si se permite el almacenamiento de cada elemento, y los controles de seguridad requeridos, por ejemplo, para proteger la confidencialidad y / o la integridad, para cada elemento de los datos durante su almacenamiento y transmisión.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
7.2 La información confidencial está protegida cuando se conserva en los sistemas del proveedor de software y se elimina de forma segura cuando ya no se necesitan.	**7.2.a** El evaluador examinará las pruebas del proveedor y entrevistará al personal para confirmar que existe un proceso sólido que garantice la protección de la información confidencial cuando se conserva en los sistemas del proveedor de software y que se eliminan de forma segura cuando ya no se necesitan.	Cuando los proveedores de software recopilan datos confidenciales de las partes interesadas, por ejemplo, para la depuración o con otros fines de apoyo al cliente, el proveedor debe coordinarlo con las partes interesadas para identificar así qué elementos de la información requieren protección. Las partes interesadas de los proveedores pueden tener su propia definición y requisitos de seguridad relacionados con la información confidencial, y ambas partes deben estar de acuerdo en cuanto a los esfuerzos de protección adecuados. Cuando el proveedor de software recopila o retiene información confidencial, debe asegurarse de que están protegidos, por ejemplo, mediante el uso de medidas sólidas de control de acceso y / o criptografía robusta con procesos de gestión claves aceptados por la industria. Tan pronto como ya no se necesiten para el propósito de la recolección, la información confidencial debe eliminarse de forma segura, de manera que no sea posible reconstruir o recuperar los datos desde ningún sistema del proveedor de software.
	7.2.b El evaluador examinará las evidencias suministradas por el proveedor y observará una muestra de los sistemas del proveedor para confirmar lo siguiente: • Que la información confidencial no reside en los sistemas de los proveedores de software a menos que existan pruebas adecuadas de aprobación y justificación. • Que la información confidencial se protege adecuadamente donde se encuentra guardada. • Que los procesos o mecanismos de borrado seguro son suficientes para hacer que la información confidencial sea irrecuperable.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Comunicaciones de Seguridad

El proveedor de software proporciona información oportuna a las partes interesadas (por ejemplo, clientes, instaladores, integradores, etc.) en relación con los problemas de seguridad que afectan a su software, así como una orientación exhaustiva sobre la implementación, configuración, funcionamiento y actualizaciones seguras del software.

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 8: Guía de Implementación del Proveedor de Software El proveedor les proporciona a las partes interesadas una orientación clara y completa sobre la implementación, configuración y funcionamiento seguros de su software.		
8.1 El proveedor de software les proporciona a las partes interesadas una orientación clara y completa sobre la implementación, configuración y funcionamiento seguros de su software.	**8.1.a** El evaluador examina las evidencias suministradas por el proveedor para confirmar lo siguiente: • Existe un proceso sólido para producir, mantener y poner a disposición de las partes interesadas orientaciones sobre la implementación, configuración y funcionamiento seguros de su software. • La guía de implementación incluye la documentación de todas las opciones y parámetros configurables relacionados con la seguridad para el software del proveedor, así como las instrucciones para configurar y asegurar adecuadamente cada una de esas opciones y parámetros.	Cuando se sigue, la guía de implementación del proveedor de software proporciona la garantía de que el software y los parches se instalen, configuren y mantengan de forma segura en el entorno del cliente, y de que todas las funciones de seguridad deseadas están activas y funcionando según lo previsto. Las orientaciones deben abarcar todas las opciones y funcionalidades disponibles para los usuarios del software que puedan afectar la seguridad del mismo o de los datos con los cuales interactúa. Las orientaciones también deben incluir opciones de configuración seguras para cualquier componente proporcionado o respaldado por el software, tal como el software externo y las plataformas subyacentes. Algunos ejemplos de Opciones Configurables incluyen: • Cambio de Credenciales y Contraseñas predeterminadas • Activación y desactivación de las cuentas, servicios y funciones de la aplicación. • Cambios en los permisos de acceso de los recursos. • Integración con las bibliotecas criptográficas de terceros, los generadores de números aleatorios, etc. Siguiendo la guía de implementación segura se debería obtener una configuración segura de todas las opciones configurables. *(continúa en la siguiente página)*
	8.1.b Para obtener una muestra del software del proveedor, examine la documentación y los materiales específicos del software para confirmar que el proveedor del software proporciona y mantiene una orientación sobre la configuración segura de cada opción o parámetro relacionado con la seguridad disponible del software del proveedor.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
8.2 La guía de implementación segura incluye las instrucciones detalladas acerca de cómo instalar, configurar y mantener de forma segura todos los componentes del software y las plataformas compatibles.	**8.2** El evaluador examina la evidencia suministrada por el proveedor para confirmar lo siguiente: • La guía de implementación segura incluye instrucciones sobre cómo instalar o iniciar, configurar y mantener el software de forma segura. • Las orientaciones de la aplicación segura son suficientemente detalladas. • Existen o se obtienen pruebas que ilustran que el seguir la guía de implementación segura resulta en una configuración de software segura.	Como se espera que el proveedor de software identifique, evalúe y gestione continuamente los riesgos de su software, los procesos de cambio del software del proveedor deben incluir la determinación del impacto del cambio en la orientación del proveedor de software. Los cambios del software que afecten a una característica u opción configurable deben dar lugar a una actualización de las directrices de la implementación segura.
8.3 La guía de implementación segura está alineada con las actualizaciones del software.	**8.3.a** El evaluador examina la evidencia suministrada por el proveedor para confirmar lo siguiente: • Que el proceso de producción y mantenimiento de las guías de implementación seguras incluye la generación de guías actualizadas cuando se publican nuevas actualizaciones del software, o se introducen o modifican las opciones o los parámetros relacionados con la seguridad. • Que las orientaciones sobre la aplicación de la seguridad se revisan al menos una vez al año para comprobar su exactitud, aunque no se publiquen las actualizaciones de las opciones y los parámetros relacionados con la seguridad.	
	8.3.b Para obtener una muestra de las actualizaciones del software, examine la guía de implementación segura, así como los detalles de las actualizaciones del software para confirmar que a medida que se actualizan o añaden las opciones y los parámetros relacionados con la seguridad, se actualiza la guía de implementación segura.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 9: Comunicaciones con las Partes Interesadas El proveedor de software mantiene canales de comunicación con las partes interesadas en cuanto a los posibles problemas de seguridad y a las opciones de mitigación.		
9.1 Los canales de comunicación se definen y se ponen a disposición de los clientes, instaladores, integradores y demás partes interesadas para que informen y reciban información sobre los problemas de seguridad y las opciones de mitigación.	**9.1** El evaluador examinará las pruebas y entrevistará al personal para confirmar lo siguiente: • Que existe un proceso sólido para apoyar las comunicaciones abiertas y bidireccionales que se tienen con las partes interesadas para informar y recibir información de seguridad acerca de los productos y servicios del proveedor de software. • Que los canales de comunicación les ofrecen a las partes interesadas la posibilidad de notificar los problemas relacionados con la seguridad y de recibir puntualmente información sobre el estado de sus consultas. • Que el proveedor de software cuenta con los recursos para responder a los informes o consultas sobre la seguridad de los productos y de los servicios del proveedor.	Que los proveedores de software deben vigilar el panorama de las amenazas para identificar las nuevas vulnerabilidades y los problemas de seguridad que afecten a su software en el mercado. Los proveedores de software también deben proporcionar líneas de comunicación abiertas para que los investigadores u otras partes interesadas puedan informar acerca de las vulnerabilidades recién descubiertas en los productos y servicios del proveedor de software. Los canales de comunicación podrían incluir una dirección de correo electrónico, una página web u otro método que facilite la interacción con los investigadores externos, por ejemplo, a través de un programa formal de recompensas por errores. El proveedor de software también debe garantizar los equipos para responder a estos informes e impulsar los procesos para corregir las vulnerabilidades del software del proveedor. Además de apoyar la recepción de la información sobre las vulnerabilidades de sus productos de software, el proveedor de software también debe emitir comunicaciones a los clientes, instaladores e integradores para proporcionarles información acerca de las vulnerabilidades conocidas y acerca de cuándo estarán disponibles las correcciones. Las correcciones o parches deben desarrollarse y publicarse de manera oportuna, basándose en la criticidad y de acuerdo con el objetivo de control 4.2. Las notificaciones de seguridad de los proveedores de software deben incluir la criticidad y el impacto potencial de la vulnerabilidad, así como una orientación clara para abordar la vulnerabilidad, —por ejemplo, cómo instalar un parche o una actualización del software. Cuando no haya una solución
9.2 Se les notifica a las partes interesadas acerca de las actualizaciones de seguridad de manera oportuna.	**9.2** El evaluador examinará las pruebas y entrevistará al personal para confirmar que existe un proceso sólido de notificación a las partes interesadas acerca de las actualizaciones de seguridad de manera oportuna.	
9.3 Cuando las actualizaciones de seguridad no están disponibles de inmediato para abordar las vulnerabilidades o explotaciones conocidas, se emiten notificaciones de seguridad a todas las partes interesadas pertinentes para proporcionarles las instrucciones para	**9.3.a** El evaluador examinará l evidencias y entrevistará al personal para confirmar que los procesos incluyen el proporcionarles a las partes interesadas las instrucciones para mitigar la amenaza, o reducir la probabilidad y / o el impacto de la explotación de los problemas de seguridad conocidos para los cuales no se proporciona el parche a tiempo.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
mitigar los riesgos asociados a las vulnerabilidades y a las fallas de seguridad conocidas.	**9.3.b** Para obtener una muestra de las actualizaciones de seguridad del software, examine las comunicaciones con las partes interesadas, la documentación específica del producto, los resultados de las pruebas de seguridad u otros materiales para confirmar que, cuando las vulnerabilidades conocidas no se abordan en las actualizaciones de seguridad, se proporcionan las instrucciones de mitigación de los riesgos a las partes interesadas.	disponible, el proveedor de software debe comunicar el riesgo y proporcionar orientación acerca de las opciones de mitigación. Las comunicaciones iniciadas por el proveedor de software podrían incluir notificaciones por correo electrónico, alertas en el sitio web, avisos por escrito, publicaciones en las redes sociales y cualquier otro canal que el proveedor mantenga para que las partes interesadas participen. Los canales de comunicación deben publicitarse para que los interesados sepan cómo acceder a estos,— por ejemplo, inscribiéndose para recibir notificaciones por correo electrónico. También debe facilitarse la información de contacto del proveedor de software para que las partes interesadas puedan formularle más preguntas acerca de las notificaciones de seguridad.

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*

Objetivos de Control	Requisitos de Pruebas	Guía
Objetivos de Control 10: Información sobre la Actualización del Software El proveedor de software les proporciona a las partes interesadas las explicaciones detalladas acerca de todos los cambios del software.		
10.1 Tras la publicación de cualquier actualización del software, se les proporciona a las partes interesadas un resumen de los cambios específicos realizados al software.	**10.1.a** El evaluador examinará las evidencias y entrevistará al personal para confirmar lo siguiente: • Existe un proceso sólido para comunicar a las partes interesadas acerca de todos los cambios del software cuando se realizan actualizaciones. • El proceso da lugar a un resumen claro y detallado de todos los cambios del software. • La información del resumen de los cambios describe claramente la funcionalidad específica del software que es afectada por los cambios. • Los detalles del cambio son fácilmente accesibles para los interesados.	Deben proporcionarse las notas de la versión para todas las actualizaciones de software, incluyendo los detalles de cualquier impacto en la funcionalidad del software y en los controles de seguridad. Informar a las partes interesadas acerca del impacto de la actualización del software les permite tomar decisiones informadas sobre si deben aplicarla y cuándo deben hacerlo.
	10.1.b Para obtener una muestra de las actualizaciones del software, el evaluador examinará la información disponible públicamente o las notificaciones relativas a las actualizaciones del software para confirmar lo siguiente: • Que la información resumida de los cambios se pone a disposición de las partes interesadas. • Que la información del resumen de cambios refleja con precisión los cambios realizados en el software.	

© 2019-2021 *PCI Security Standards Council, LLC. Todos los derechos reservados.*