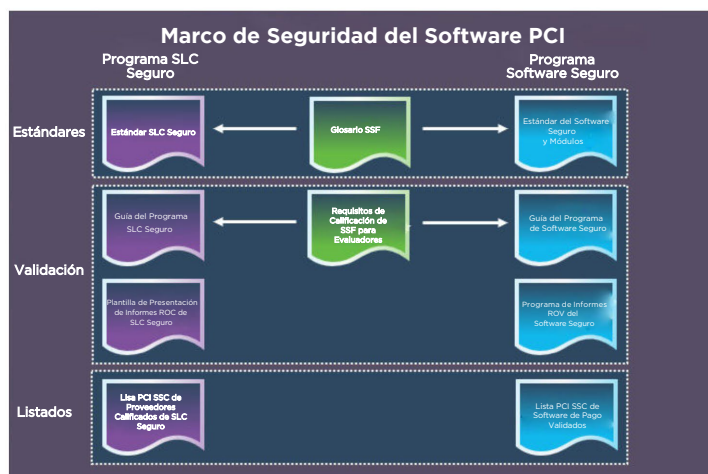


El Marco de Seguridad del Software PCI Proporciona un Enfoque Moderno para la Seguridad del Software de Pago

El Marco de Seguridad del Software (SSF) de PCI es una colección de estándares y programas para el diseño y desarrollo seguros de software de pago. La seguridad del software de pago es una parte crucial del flujo de las transacciones de pago y es esencial para facilitar transacciones de pago fiables y precisas. El SSF sustituye al Estándar de Seguridad de Datos de Aplicaciones de Pago (PA-DSS) con unos requisitos modernos que apoyan una gama más amplia de tipos de software de pago, tecnologías, y metodologías de desarrollo. Con sus requisitos centrados en los resultados, el SSF proporciona más agilidad para que los desarrolladores incorporen la seguridad en las aplicaciones de pago con prácticas de desarrollo ágiles y ciclos de actualización frecuentes. El SSF permite acelerar la personalización y características de las aplicaciones de pago para los comerciantes sin comprometer la seguridad. También mejora la coherencia y la transparencia en las pruebas de las aplicaciones de pago, lo que eleva la garantía de validación para los comerciantes, proveedores de servicios, y adquirentes que implementan y manejan el uso de soluciones de pago. Este resumen proporciona una visión general y describe la importancia del SSF, sus beneficios para las partes interesadas del sector de los pagos y cómo se utiliza.



Beneficios del Marco

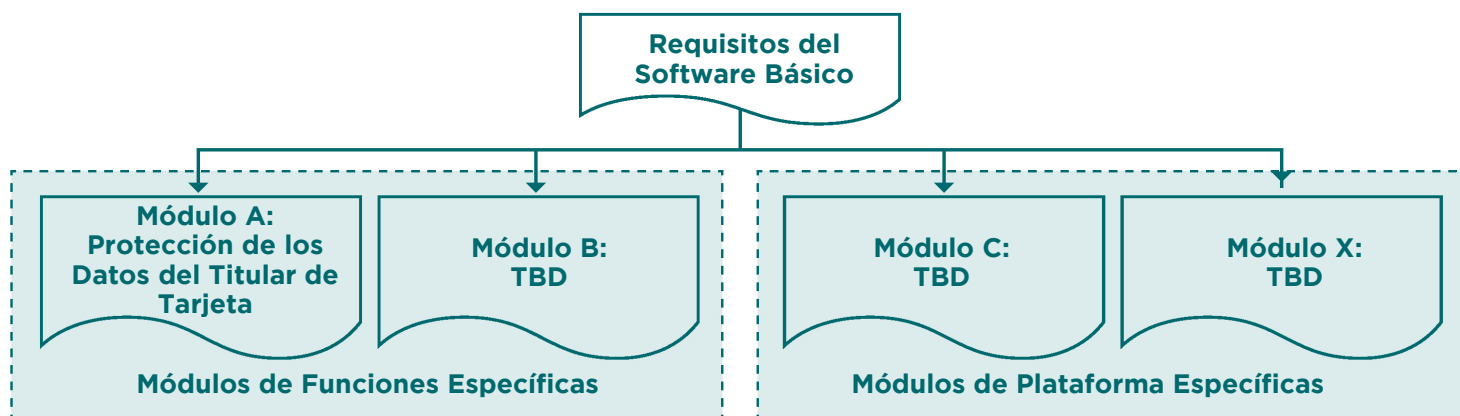
- Proporciona un nuevo enfoque para validar la seguridad del software de pago tradicional moderno y futuro
- Promueve la educación del desarrollador sobre la importancia de integrar la seguridad en el ciclo de vida del desarrollo del software
- Apoya procesos de desarrollo de software ágil y metodologías
- Ofrece flexibilidad para los Proveedores Cualificados de SLC Seguro para manejar los cambios delta del Software de Pago Validados
- Proporciona listas autorizadas de Software de Pago Validado y Proveedores de SLC Seguro Cualificado en el sitio web PCI SSC

Requisitos Flexibles y Opciones de Validación que Apoyan una Gama más Amplia de Software de Pago

El desarrollo moderno de software requiere una seguridad centrada en objetivos de apoyo a los ciclos de desarrollo y actualización más ágiles que las prácticas tradicionales de desarrollo de software. El Marco de Seguridad del Software PCI (SSF) reconoce esta evolución con un enfoque que apoya tanto el software de pago tradicional como el moderno. Proporciona una nueva metodología para validar la seguridad del software y una cualificación independiente del ciclo de vida del software seguro para los proveedores con prácticas robustas de desarrollo de seguridad.

SSF funciona de manera similar al programa PA-DSS. Los Evaluadores del Marco de Software Seguro (Evaluadores SSF) evalúan a los proveedores y sus productos de software de pago con respecto al Estándar del Ciclo de Vida de Software Seguro (SLC Seguro) y el Estándar de Software Seguro, respectivamente. El PCI SSC enumera tanto a los Proveedores Cualificados de SLC Seguro como el Software de Pago Validado en el sitio web del Consejo como recursos para comerciantes, proveedores de servicios y adquirentes. A medida que se añadan nuevos módulos al Estándar de Software Seguro para abordar otros tipos de software, casos de uso y tecnologías, el alcance del programa se ampliará para apoyarlos.

Estándar del Software Seguro



Conceptualmente, la arquitectura basada en módulos del Estándar de Software Seguro se compone de requisitos básicos del software de pago, apoyados por módulos de funciones específicas y plataformas para abordar casos de uso particulares. Los procedimientos de validación están previstos en los Programas asociados al Estándar de Software Seguro y el Estándar SLC de Software Seguro, que son seguidos por los Evaluadores SSF.

Estándar del Software Seguro

El Estándar de Software Seguro proporciona los requisitos de seguridad para construir un software de pago seguro que proteja la integridad y la confidencialidad de los datos sensibles que se almacenan, procesan o transmiten en asociación con las transacciones de pago. Está destinado a proveedores que desarrollan software de pago que apoya o facilita las transacciones de pago.

Programa de Software Seguro

La validación del Estándar de Software Seguro muestra que el producto del software de pago está diseñado, diseñado, desarrollado y mantenido de una manera que protege las transacciones y los datos de pago, minimiza las vulnerabilidades y defiende contra los ataques.

Luego de la evaluación exitosa por parte de un Evaluador de Software Seguro, el software de pago validado se reconocerá en la Lista PCI SSC de Software de Pago Validado, que reemplazará la actual Lista de Aplicaciones de Pago Validadas cuando PA-DSS se retire a fines de octubre de 2022. Hasta entonces, PCI SSC continuará manteniendo el Programa PA-DSS y la lista, lo que incluye respetar las fechas de vencimiento de validación existentes hasta final de octubre de 2022 y aceptar las nuevas presentaciones PA-DSS hasta el 30 de junio de 2021.

Evaluadores del Marco de Seguridad del Software (Evaluadores SSF)

PCI SSC cualifica a compañías e individuos dentro de esas compañías para realizar evaluaciones SSF. La cualificación del Evaluador SSF de la Compañía está abierta a cualquier compañía que cumpla con los requisitos de cualificación. Las compañías pueden cualificar para realizar evaluaciones de SLC Seguro, evaluaciones de Software Seguro o ambas. Para figurar como una Compañía Evaluadora SSF en el sitio web PCI SSC, la compañía debe tener al menos un empleado que complete con éxito el entrenamiento y el examen de Evaluador de Software Seguro o Evaluador de SLC Seguro. Para obtener información adicional, consulte el [Marco de Seguridad del Software - Requisitos de Cualificación para Evaluadores](#).

Para obtener información y recursos específicos para ayudar con la migración a SSF desde PA-DSS, consulte esta Guía de Recursos PCI SSC: [Transición de PA-DSS al Marco de Seguridad del Software PCI](#).

Estándar del Ciclo de Vida de Software Seguro (SLC Seguro)

El Estándar SLC Seguro proporciona requisitos de seguridad para que los proveedores de software de pago integren la seguridad a lo largo de todo el ciclo de vida del software, lo que da como resultado un software que es seguro por diseño y capaz de resistir los ataques. Está destinado a proveedores que están desarrollando software de pago para apoyar o facilitar las transacciones de pago.

Programa SLC Seguro

La validación del Estándar SLC Seguro ilustra que el proveedor de software cuenta con prácticas seguras de gestión del ciclo de vida del software para garantizar que su software de pago esté diseñado, desarrollado y mantenido para proteger las transacciones y los datos de pago, minimizar las vulnerabilidades y defenderse de los ataques.

Luego de la validación exitosa por parte de un Evaluador de SLC Seguro, los proveedores de software serán reconocidos en la Lista PCI SSC de Proveedores Cualificados de SLC Seguro. Podrán certificar por sí mismos los cambios delta para cualquiera de sus productos enumerados como Software de Pago Validado bajo el Programa de Software Seguro y desarrollado utilizando el proceso SLC validado.