Descripción del servicio

Estándar de seguridad de datos de la aplicación de pago

Servicio de validación de cumplimiento

Contenido

Servicio de validación de cumplimiento del PA-DSS

SecureTrust™ es una división de Trustwave Holdings, Inc.

DESCRIPCIÓN DEL SERVICIO

El Servicio de validación de cumplimiento (Compliance Validation Service, CVS) del Estándar de seguridad de datos de las aplicaciones de pago (Payment Application Data Security Standard, PA-DSS) (el "**Servicio**") se diseñó para validar si los controles y las operaciones de seguridad de la aplicación de pago que se han identificado han logrado cumplir con el PA-DSS conforme a lo establecido por el Consejo de Estándares de Seguridad del Sector de las Tarjetas de Pago (Payment Card Industry, PCI) (el "**Estándar**"). El Servicio consiste en una evaluación del diseño y de la implementación de los controles y la política, los procedimientos y las prácticas del PA-DSS que son relevantes para el Estándar.

Los términos en mayúscula que se utilizan en esta descripción del servicio, pero que no se definen en el presente documento, tienen el significado que se asignó en el Acuerdo maestro de servicios de Trustwave que se encuentra en https://www.trustwave.com/en-us/legal-documents/contract-documents/ o en un acuerdo similar celebrado entre SecureTrust y el Cliente.

CARACTERÍSTICAS BÁSICAS DEL SERVICIO

El Servicio incluye las siguientes características básicas:

Portal de SecureTrust

Una de las características del Portal de SecureTrust consta de, entre otras, la aplicación Compliance Manager para gestionar el proceso de cumplimiento, así como para recopilar y almacenar de forma segura las pruebas, la documentación y los productos finales.

Servicios globales de riesgo y cumplimiento

El equipo de Servicios Globales de Riesgo y Cumplimiento (Global Compliance and Risk Services, GCRS) está formado, entre otros, por los siguientes cargos y funciones clave:

Asesor de seguridad calificado de la aplicación de pago (Payment Application Qualified Security Assessor, PA QSA): el PA QSA es el principal recurso para el cumplimiento del Servicio, y es responsable de realizar la evaluación, la determinación de cumplimiento y la elaboración de informes.

Consultor de gestión (Managing Consultant, MC): el MC brinda orientación, supervisa los proyectos e informa acerca de la gestión de calidad al PA QSA, además de actuar como punto de contacto secundario del Cliente en lo que respecta a derivaciones y consultas.

Comité de Revisión de Cumplimiento (Compliance Review Board, CRB): actúa como la autoridad final para la interpretación de los requisitos del Estándar o la resolución de inquietudes de cumplimiento complejas, al proporcionar uniformidad y continuidad en todas las evaluaciones de SecureTrust. El CRB también es

la autoridad final de derivación para la resolución de problemas relacionados con el estado de cumplimiento de los requisitos del Estándar o la revisión de un control compensatorio.

CVS del PA-DSS: el Servicio valida si los controles y las operaciones de seguridad de la aplicación de pago del Cliente que se han identificado han logrado cumplir con el Estándar. Si se determina que la aplicación del cliente cumple con el Estándar, SecureTrust le proporcionará un Informe de validación (Report of Validation, ROV) a modo de declaración del estado de cumplimiento del Cliente. Si se determina que la aplicación del cliente no cumple con el Estándar, SecureTrust le proporcionará un ROV de incumplimiento en el que se detallarán los resultados del Servicio.

PRESTACIÓN E IMPLEMENTACIÓN

Inicio del proyecto

El equipo de GCRS de SecureTrust facilita la prestación del Servicio, lo que incluye programar y llevar a cabo la reunión remota inicial para definir y acordar un plan de proyecto de alto nivel que cuente con fechas cruciales, pasos clave, estimaciones de duración, productos finales, requisitos de recursos y procedimientos de derivación.

Fase I: recopilación de información

SecureTrust y el Cliente colaborarán para recopilar y analizar la información de la aplicación del Cliente. SecureTrust llevará a cabo entrevistas, según sea necesario, con arquitectos de sistemas, desarrolladores de aplicaciones, desarrolladores de bases de datos, administradores de sistemas, personal de gestión de calidad (Quality Assurance, QA) o personal de pruebas, y otros miembros del personal del Cliente que puedan proporcionar detalles relevantes sobre la aplicación.

Algunos temas relevantes para la recopilación de información son, entre otros, los siguientes:

- Una descripción de la aplicación del Cliente a fin de tener una comprensión básica de dicha aplicación.
- El nombre y número de versión de la aplicación, así como los sistemas operativos compatibles y cualquier requisito de hardware o software.
- Una descripción de los componentes que conforman la aplicación del Cliente.
- Una lista de hardware y software necesarios para ejecutar la aplicación del Cliente, incluida cualquier dependencia de terceros, según corresponda.
- Una descripción de la función que cumple la aplicación en el proceso de pago, incluidas las funciones de autorización y transacción, según corresponda.
- Los procesos del ciclo de desarrollo del software (Software Development Lifecycle, SDLC).
- Las especificaciones de diseño funcional que demuestran el diseño de la aplicación del Cliente y las implementaciones funcionales.
- Las operaciones de gestión clave, incluida cualquier integración con funciones de cifrado de terceros, según corresponda.
- La documentación y los diagramas de la interfaz de la aplicación del Cliente que ilustran los flujos de datos internos y externos, incluida la comunicación de red interna y externa, según corresponda.
- Una lista de las herramientas de prueba de la aplicación que podrían ser necesarias para las pruebas de laboratorio.
- Una descripción de los comandos de prueba de la aplicación de pago y la documentación del entorno de prueba de la aplicación para el tratamiento de datos, según corresponda.

- La documentación de implementación del Cliente, lo que incluye las recomendaciones y los procedimientos seguros para la integración de la aplicación en los entornos comerciales.

Es posible que SecureTrust requiera una demostración remota de la aplicación del Cliente a fin de determinar qué pruebas se necesitarán para completar la fase de revisión de la aplicación del CVS del PA-DSS, según se describe a continuación.

Fase II: revisión de la aplicación

El Servicio de la fase de revisión de la aplicación se llevará a cabo en los laboratorios de prueba de SecureTrust o en las instalaciones del Cliente, según las restricciones logísticas y la naturaleza y los sistemas necesarios para la aplicación del Cliente. SecureTrust colaborará con el Cliente para determinar si es necesaria una visita in situ o si las pruebas se pueden llevar a cabo en los laboratorios de prueba de SecureTrust.

La fase de revisión de la aplicación se enfoca en el análisis lógico de la aplicación del Cliente según los requisitos establecidos en el Estándar. Esta fase también incluye cualquier entrevista o revisión de documentación restante, así como cualquier observación del proceso in situ. SecureTrust conocerá en su totalidad la forma en que la aplicación del Cliente trata los datos, la forma en que se desarrolló, distribuyó y configuró, y la forma en que está protegida de accesos no autorizados.

SecureTrust examinará el entorno de ejecución del Cliente, incluida la revisión de las herramientas, las funciones y los componentes de software y hardware, las bibliotecas de código abierto y de terceros, los requisitos y las dependencias, según corresponda.

SecureTrust examinará los parámetros críticos de la aplicación del Cliente, como los procesos de tratamiento de datos, los esquemas de bases de datos y las condiciones de error. También es posible que SecureTrust verifique los procesos escritos de desarrollo de software del Cliente, revise las configuraciones, la producción y los datos de prueba relevantes de la aplicación, las características de autenticación, los controles de cambios, el almacenamiento y cifrado de datos, el registro de auditorías y las características de mantenimiento. Además, realizará una prueba funcional de los controles, según corresponda, para determinar que la aplicación del Cliente cumpla con el Estándar.

SecureTrust colaborará con el Cliente para resolver las preguntas de evaluación del Cliente y le proporcionará asistencia razonable en la interpretación del Estándar y sus respuestas. Es posible que SecureTrust solicite una revisión adicional de la aplicación del Cliente, las áreas de código aplicables, la documentación o los procesos y procedimientos de tratamiento de datos.

SecureTrust llevará a cabo una prueba de penetración de la aplicación de forma remota o en sus laboratorios de pruebas. En la prueba se determinará el grado de seguridad de la aplicación del Cliente con respecto a vulnerabilidades comunes y otras vulnerabilidades mencionadas en el Estándar, según corresponda. SecureTrust le proporcionará al Cliente un informe en el que se detallarán los resultados de la prueba de penetración de la aplicación, incluido cualquier paso de corrección que se requiera para que la aplicación del Cliente logre el cumplimiento del Estándar. En el caso de las aplicaciones basadas en la web, se debe realizar una prueba detallada para determinar el estado de cumplimiento de la aplicación del Cliente, la cual no se incluye como parte del Servicio.

Fase III: elaboración de informes

SecureTrust elaborará un informe donde se documentarán observaciones y recomendaciones del Servicio.

El informe preliminar se enviará al Cliente para que lo revise. El Cliente puede comentar o sugerir cambios en el informe preliminar y la documentación de respaldo antes de que el equipo de QA de SecureTrust finalice el informe. SecureTrust tiene la autoridad final respecto del contenido del informe definitivo y el tipo de producto final que se producirá.

SecureTrust proporcionará un informe del producto final, tal como se define a continuación:

- Si se determina que la aplicación del Cliente cumple con el Estándar, y una vez que el equipo de QA de SecureTrust lo finalice, se presentará el ROV, junto con la documentación de respaldo necesaria, al Consejo de Estándares de Seguridad del Sector de Tarjetas de Pago (Payment Card Industry Security Standards Council, PCI SSC) para considerar su inclusión.
- Si se determina que la aplicación no cumple con el Estándar, SecureTrust le proporcionará al Cliente un ROV de incumplimiento.

SecureTrust llevará a cabo una reunión de cierre con el Cliente.

RESPONSABILIDADES DE SECURETRUST

- Establecer contacto y permanecer a disposición para las comunicaciones con el Cliente.
- Establecer planes de comunicación y derivación.
- Crear una cuenta de Cliente en el Portal de SecureTrust.
- Definir un plan de proyecto de alto nivel que contenga fechas cruciales, pasos clave, estimaciones de duración, productos finales y requisitos de recursos.
- Programar y llevar a cabo reuniones iniciales, periódicas de seguimiento y de cierre.
- Validar el alcance del Servicio.
- Crear y aplicar las tareas pendientes del Cliente en la aplicación Compliance Manager del Portal de SecureTrust.
- Entrevistar al personal correspondiente de la organización y recopilar información al respecto.
- Realizar una validación de conformidad con los procedimientos de prueba del PA-DSS.
- Proporcionar al Cliente información sobre cualquier observación que requiera una corrección.
- Determinar los resultados del Servicio y el estado de cumplimiento de la aplicación al finalizar el Servicio.
- Producir un ROV de cumplimiento o incumplimiento del PA-DSS, según el estado de la aplicación en el momento de la prestación del Servicio.
- Entregar al Cliente un informe final en el que se documenten observaciones y recomendaciones del Servicio.

RESPONSABILIDADES Y CONFIRMACIONES DEL CLIENTE

- Establecer contacto y permanecer a disposición para las comunicaciones con SecureTrust.
- Establecer planes de comunicación y derivación.
- Acordar un plan de proyecto de alto nivel que contenga fechas cruciales, pasos clave, estimaciones de duración, productos finales y requisitos de recursos.
- Proporcionar de forma precisa toda la información necesaria, lo que incluye las partes interesadas clave, la información correspondiente del entorno del Cliente y los requisitos de configuración.
- Informar a SecureTrust acerca de todas las actividades de mantenimiento del entorno del Cliente y los cambios que podrían afectar el Servicio.
- Responder con precisión a las solicitudes de los equipos de SecureTrust al establecer contacto y recopilar información.

- Proporcionar detalles completos y precisos del entorno relevante y otros datos de las operaciones comerciales.
- Poner a disposición recursos capaces de participar en las actividades de evaluación de cumplimiento.
- Participar en la explicación de los materiales durante las llamadas, las reuniones, las entrevistas, los debates, la inspección de instalaciones y los análisis de controles, y comprenderlos.
- Confirmar lo siguiente:
    - Todas las actualizaciones de seguridad y las características del software del Portal de SecureTrust se incluirán en las actualizaciones de versiones más importantes.
    - El Servicio usa como referencia los requisitos y procedimientos de prueba del Estándar vigente aplicable al momento de la fecha de inicio del servicio.
    - El Servicio puede constar de actividades de evaluación remotas e in situ.
    - El Servicio comenzará el día de la llamada inicial. El plazo y la finalización del Servicio se determinarán durante la llamada inicial.
    - El Cliente debe presentar la documentación y las pruebas solicitadas por SecureTrust en un plazo de cuarenta y cinco (45) días a partir del inicio del Servicio.
        - El Cliente debe presentar todas las pruebas y llevar a cabo las actividades de corrección antes de los cuarenta y cinco (45) días previos a la finalización del Servicio.
    - La revisión de la documentación incluye una revisión inicial de la documentación del Cliente con comentarios directos relacionados con las observaciones de incumplimiento, y una revisión de la documentación corregida del Cliente.
    - El Servicio incluye una evaluación de la aplicación.
    - Los preparativos del laboratorio son responsabilidad del Cliente. El Cliente debe proporcionar un laboratorio para llevar a cabo las pruebas de la aplicación que cumpla con los controles del Estándar de seguridad de datos del PCI (PCI DSS), de conformidad con el Apéndice B del Estándar. Si las pruebas se llevan a cabo en el laboratorio de SecureTrust, el Cliente debe proporcionar sistemas que estén configurados de conformidad con el PA DSS y el PCI DSS.
    - Cuando las pruebas se lleven a cabo en el laboratorio de SecureTrust, siempre que sea posible, la empresa proporcionará la infraestructura necesaria para ejecutar los sistemas del Cliente. Si el Cliente ha optado por llevar a cabo las pruebas en el laboratorio de SecureTrust y sus sistemas requieren licencias, conectores o hardware especiales, deberá proporcionar los componentes del sistema necesarios para que se puedan realizar las pruebas, y deberá responsabilizarse por los costos relacionados. SecureTrust no comprará licencias de sistemas operativos ni ninguna otra licencia necesaria para poner a prueba las aplicaciones del Cliente, de conformidad con los requisitos relacionados con el entorno de prueba de la aplicación del PA-DSS. El Cliente proporcionará un lugar, una licencia, una autorización de función de prueba especial y otras formas de acceso autorizado a SecureTrust en caso de que este deba utilizar alguna de las aplicaciones relevantes del Cliente.
    - SecureTrust puede solicitar pruebas de los sistemas y procesos del Cliente, según sea necesario, para evaluar el cumplimiento de cualquier requisito específico. El Cliente proporcionará todas estas pruebas de manera oportuna.

    - SecureTrust no es responsable de definir los sistemas dentro del alcance ni de establecer si la información proporcionada por el Cliente es precisa.

- SecureTrust se reserva el derecho de rechazar o aceptar los comentarios del Cliente en función de los hechos y las circunstancias del Servicio.
- SecureTrust brindará el Servicio en el idioma inglés.
- SecureTrust no creará ni modificará la documentación del Cliente como parte del Servicio.
- SecureTrust no proporcionará servicios de corrección como parte del Servicio.
- SecureTrust no ofrecerá orientación ni asesoramiento legal.
- La calidad y la precisión del Servicio dependerán de que el Cliente proporcione a SecureTrust información precisa y acceso a sus sistemas y recursos.