Descripción del servicio

Estándar de seguridad de datos del sector de tarjetas de pago

Evaluación de deficiencias

Contenido

Evaluación de deficiencias del PCI DSS

SecureTrust™ es una división de Trustwave Holdings, Inc.

DESCRIPCIÓN DEL SERVICIO

La evaluación de deficiencias del Estándar de seguridad de datos del sector de tarjetas de pago (Payment Card Industry Data Security Standard, PCI DSS) (el "Servicio") se diseñó para identificar deficiencias y priorizar las áreas que podrían requerir una corrección para cumplir con el PCI DSS conforme a lo establecido por el Consejo de Estándares de Seguridad del PCI (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 (Qualified Security Assessor, 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): brinda orientación, supervisa los proyectos e informa acerca de la gestión de calidad al 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.

Evaluación de deficiencias: la evaluación identifica deficiencias y prioriza las áreas que podrían requerir una corrección para lograr cumplir con el Estándar. SecureTrust le proporcionará al Cliente orientación para el diseño de los controles del PCI DSS y la identificación de la política, los procedimientos y las

prácticas organizacionales de respaldo que son relevantes para el Estándar. SecureTrust le proporcionará un informe final donde 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 acerca de los sistemas dentro del alcance del Cliente.

SecureTrust trabajará con el Cliente, cuando corresponda, para hacer lo siguiente:

- Determinar activos críticos.
- Evaluar procesos comerciales.
- Identificar los procesos de gestión del cumplimiento y la seguridad implementados.
- Revisar la documentación de cumplimiento del PCI DSS previa.

Fase II: evaluación de deficiencias del PCI DSS

SecureTrust llevará a cabo revisiones de documentación, entrevistas, debates, revisiones de pruebas, inspecciones de instalaciones, análisis de controles y evaluaciones de la arquitectura de seguridad actual del Cliente.

SecureTrust trabajará con el Cliente, cuando corresponda, para hacer lo siguiente:

- Evaluar la idoneidad del conocimiento del Cliente acerca del Estándar y las responsabilidades de todas las partes involucradas para demostrar que se cumple con el PCI DSS.
- Lograr un entendimiento del entorno para identificar deficiencias críticas entre el estado actual del Cliente y el Estándar.
- Lograr un entendimiento de la postura de cumplimiento del Cliente con respecto al PCI DSS.
- Identificar deficiencias para cumplir con el Estándar.
- Priorizar los esfuerzos de corrección necesarios para cumplir con el Estándar.

SecureTrust analizará las pruebas de conformidad con el Estándar y determinará el estado de cumplimiento de los sistemas dentro del alcance del Cliente.

Fase III: elaboración de informes

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

Se enviará un informe preliminar al Cliente para que lo revise. El Cliente podrá comentar o sugerir cambios en el informe preliminar antes de que el equipo de Gestión de Calidad (Quality Assurance, QA) de SecureTrust finalice el informe. SecureTrust tiene la autoridad final respecto del contenido del informe y el tipo de producto final a producir.

SecureTrust proporcionará un informe definitivo como producto final.

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, incluida la segmentación, y analizar la metodología de muestreo.
- Crear y aplicar las tareas pendientes del Cliente dentro la aplicación Compliance Manager del Portal.
- Entrevistar al personal correspondiente de la organización y recopilar información al respecto.
- Realizar una evaluación de deficiencias con respecto a los procedimientos de pruebas del Estándar.
- Determinar los resultados del Servicio de conformidad con el Estándar.
- Crear un informe preliminar al momento de la evaluación.
- Entregar al Cliente un informe final en el que se documentarán observaciones y recomendaciones de la evaluación.

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 del Servicio.
- 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 no reemplazará una evaluación de validación de cumplimiento del PCI DSS y no derivará en un informe o un certificado de cumplimiento.
    - El Servicio puede constar de actividades de evaluación remotas e in situ.
    - Las fechas de inicio y finalización del proyecto se determinarán durante la llamada inicial.
    - SecureTrust puede solicitar pruebas de los sistemas y los procesos del Cliente, según sea necesario, para demostrar el cumplimiento con cualquier requisito específico. El Cliente acepta presentar todas las pruebas de forma 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.