# Descripción del servicio

## Estándar de seguridad de datos del sector de tarjetas de pago

## Servicio de validación de cumplimiento

# Contenido

# SERVICIO DE VALIDACIÓN DE CUMPLIMIENTO DEL PCI 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 del sector de tarjetas de pago (Payment Card Industry Data Security Standard, PCI DSS) (el "**Servicio**") incluye servicios profesionales que ayudan a validar si los componentes del sistema incluidos o conectados al entorno de datos del titular de la tarjeta (Cardholder Data Envirnoment, CDE) del Cliente cumplen con el PCI DSS, en virtud de lo establecido por el Consejo de Estándares de Seguridad del PCI (el "Estándar"). El Servicio también incluye el acceso al Portal de SecureTrust con aplicaciones para gestionar el proceso de cumplimiento y administrar los escaneos de vulnerabilidad externa del PCI.

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

Las funciones del Portal de SecureTrust consisten, entre otras cosas, en las siguientes aplicaciones y funciones clave:

Compliance Manager: la aplicación para gestionar el proceso de cumplimiento, así como para recopilar y almacenar de forma segura las pruebas, la documentación y los productos finales.

PCI Manager: la aplicación para gestionar escaneos ilimitados de la vulnerabilidad externa del PCI con un escáner certificado de un proveedor de escáneres aprobado (Approved Scanning Vendor, ASV), y para generar informes de escaneos del ASV para el PCI.

### 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 validación, 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.

CVS del PCI DSS: el Servicio valida si los componentes del sistema identificado incluidos o conectados al CDE cumplen con el Estándar. Si se determina que los sistemas dentro del alcance del Cliente cumplen con el Estándar, SecureTrust le proporcionará un informe de cumplimiento (Report of Compliance, ROC) y un certificado de cumplimiento (Attestation of Compliance, AOC) como declaración de su estado de cumplimiento. Si se determina que los sistemas del Cliente dentro del alcance no cumplen con el Estándar, SecureTrust le proporcionará un ROC de incumplimiento.

Gestión de Calidad (Quality Assurance, QA) de SecureTrust: el equipo de QA de SecureTrust evalúa el ROC y controla los hallazgos antes de la presentación formal, tal como lo requiere el Consejo de Estándares de Seguridad del PCI. Una vez completada la evaluación del ROC, el equipo de QA de SecureTrust finalizará el ROC y el AOC para entregárselos al Cliente o a las entidades generadores de informes relevantes.

Reuniones de revisión habituales (Business-as-Usual, BAU): se llevan a cabo durante el año para supervisar y revisar la efectividad de los procesos de control de seguridad del Cliente al momento de mantener el cumplimiento con el PCI DSS de forma continua. SecureTrust le acordará con el Cliente reuniones de revisión BAU trimestrales.

Puntuaciones de madurez de la seguridad: identifican las tasas de madurez de la organización del Cliente y ayudan a priorizar áreas que podrían necesitar correcciones, para lograr el cumplimiento con el nivel de madurez necesario para que el Cliente implemente los controles del PCI DSS.

# 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.

Algunas actividades de recopilación de información clave son las siguientes:

- Recopilación de documentación sobre el alcance.

    - La documentación sobre el alcance puede incluir políticas y procedimientos, inventarios de activos, diagramas de flujo de datos, diagramas de redes y otra documentación que defina a los sistemas dentro del alcance del Cliente.
- Acuerdo con respecto a los sistemas iniciales dentro del alcance.
- Identificación de medidas iniciales o pruebas faltantes.

SecureTrust realizará una verificación de la disposición para el PCI con el fin de determinar la capacidad del Cliente de completar el Servicio. Si la verificación de la disposición para el PCI determina que el Cliente no está listo para completar el Servicio o no cumple con el Estándar, pero se requiere una declaración oficial sobre el cumplimiento, SecureTrust le proporcionará un ROC de incumplimiento.

## Fase II: pruebas

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 recopilará pruebas a través de las tareas pendientes en la aplicación Compliance Manager que se encuentra en el Portal de SecureTrust.

SecureTrust determinará si los sistemas dentro del alcance del Cliente son aptos para muestreo. Si los sistemas dentro del alcance del Cliente son aptos para muestreo y los conjuntos de muestras identifican elementos que no cumplen con el Estándar, se recolectará un segundo conjunto de muestras. Si el segundo conjunto de muestras también identifica elementos que no cumplen con el Estándar, los sistemas dentro del alcance del Cliente se identificarán como incumplidores.

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 ROC del PCI DSS 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 definitivo, tal como se define a continuación:

- Si se determina que los sistemas dentro del alcance del Cliente cumplen con el Estándar, y una vez que el equipo de QA de SecureTrust lo finalice, se presentará el ROC, junto con la documentación de respaldo necesaria, al punto de contacto del Cliente o a las entidades generadoras de informes relevantes.
- Si se determina que los sistemas del Cliente dentro del alcance no cumplen con el Estándar, SecureTrust le proporcionará un ROC de incumplimiento.

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

## Reuniones de revisión BAU

SecureTrust llevará a cabo Reuniones de revisión BAU trimestrales durante el plazo del Servicio.

SecureTrust completará y entregará una hoja de cálculo de “Revisión BAU” al punto de contacto del Cliente por cada reunión de revisión BAU.

### Puntuaciones de madurez de la seguridad

SecureTrust llevará a cabo la puntuación de madurez de la seguridad como parte del Servicio.

Le proporcionará al Cliente las puntuaciones de madurez de la seguridad para que implemente los controles y las categorías de control de seguridad del PCI DSS.

## 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 pasos clave, estimaciones de duración, productos finales y requisitos de recursos.
- Programar y llevar a cabo reuniones iniciales, periódicas de seguimiento y de cierre.
- Llevar a cabo la verificación de disposición para el PCI.
- Validar el alcance del Servicio, incluida la segmentación, y analizar la metodología de muestreo.
- Crear y aplicar las tareas pendientes en la aplicación Compliance Manager del Portal de SecureTrust.
- Determinar la elegibilidad para muestreo del Cliente.
- Realizar una validación de conformidad con los procedimientos de pruebas del Estándar.
- Identificar ante el Cliente cualquier observación que requiera corrección.
- Determinar el estado de cumplimiento de los sistemas dentro del alcance del Cliente, de conformidad con el Estándar.
- Producir un ROC de cumplimiento o incumplimiento del PCI DSS, según el estado de los sistemas dentro del alcance del Cliente al momento de la prestación del Servicio.
- Entregar al Cliente un informe final en el que se documenten observaciones y recomendaciones del Servicio.
- Llevar a cabo reuniones de revisión BAU.
- Realizar puntuaciones de madurez de la seguridad.

## 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.
- Acordar las fechas de inicio y finalización del Servicio.
- Presentar todas las pruebas y completar las actividades de corrección antes de los cinco (5) días previos a la finalización del Servicio.
- 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 puede constar de actividades de evaluación remotas e in situ.
    - Las fechas de inicio y finalización del Servicio 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.