Descripción del servicio

Consultoría general sobre el PCI PIN

Contenido

Consultoría general sobre el PCI PIN

SecureTrust™ es una división de Trustwave Holdings, Inc.

DESCRIPCIÓN DEL SERVICIO

El servicio de consultoría general sobre el Número de identificación personal del sector de tarjetas de pago (Payment Card Industry Personal Identification Number, PCI PIN) de SecureTrust es un servicio de consultoría (el "**Servicio**") para el diseño de las soluciones, el diseño de las aplicaciones, las políticas, los procedimientos y las prácticas que emplea la organización para cumplir con los requisitos de seguridad del PCI PIN y la Guía del programa del asesor de PIN calificado (Qualified PIN Assessor, QPA), o que se destinan al uso por parte de la organización, 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 PIN calificado (QPA): es el principal recurso para el cumplimiento del Servicio y es responsable de realizar las actividades de consultoría.

Consultor de gestión (Managing Consultant, MC): brinda orientación, supervisa los proyectos e informa acerca de la gestión de calidad al QPA, 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 de seguridad del PCI PIN, versión 3 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.

Consultoría general sobre el PCI PIN: el QPA de SecureTrust le ofrece al cliente servicios de consultoría general acerca de la interpretación de los requisitos, los desafíos de cumplimiento, el diseño de soluciones o aplicaciones, las políticas, los procedimientos y otros temas relacionados con el Estándar. El QPA puede ayudar a analizar las operaciones y las salvaguardas de seguridad del PCI PIN existentes o planificadas del Cliente por medio de servicios de consultoría in situ o remotos.

PRESTACIÓN E IMPLEMENTACIÓN

Inicio del proyecto

El equipo de GCRS de SecureTrust inicia el Servicio al programar y llevar a cabo una 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.

SecureTrust solicitará información inicial y programará reuniones futuras. El Cliente proporcionará un resumen preliminar de su entorno de PCI PIN.

Fase I: recopilación de información

SecureTrust y el Cliente colaborarán para recopilar y analizar la información del entorno de PCI PIN del Cliente.

SecureTrust evaluará la documentación del diseño aplicable para comprender la funcionalidad, los procesos de tratamiento de datos y los parámetros de diseño del entorno de PCI PIN del Cliente.

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

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

Fase II: consultoría general sobre el PCI PIN

El Servicio puede prestarse in situ dentro de las instalaciones del cliente, o puede proporcionarse de forma remota, a discreción de SecureTrust. Un QPA de SecureTrust trabajará con el Cliente para determinar las áreas del Estándar en que deberían enfocarse.

SecureTrust proporcionará consultoría alrededor de las áreas acordadas con el Cliente que se relacionen con su entorno de PCI PIN. La consultoría se realizará de conformidad con lo establecido en el Estándar, y se analizarán los requisitos de pruebas y su aplicabilidad en el entorno del Cliente.

Algunas actividades del Servicio son las siguientes:

- Revisar políticas y procedimientos.
- Evaluar las configuraciones del sistema.
- Realizar entrevistas.
- Observar los procesos y procedimientos realizados de conformidad con la documentación recopilada durante la fase de recopilación de información.
- Realizar inspecciones físicas de las instalaciones y los equipos.
- Identificar y realizar una revisión de alto nivel de los terceros utilizados para respaldar el entorno de PCI PIN del Cliente.

- Prestar servicios de consultoría acerca de los requisitos de PCI PIN específicos.

SecureTrust colaborará con el Cliente para resolver las preguntas que tenga acerca de la evaluación. SecureTrust también le proporcionará al Cliente asistencia razonable para la interpretación del Estándar y de sus respuestas. Es posible que SecureTrust solicite una revisión adicional del entorno de PCI PIN, la documentación, o los procesos y procedimientos de tratamiento de datos del Cliente.

El Servicio no está destinado a enfocarse en ningún control específico, a menos que SecureTrust y el Cliente lo acuerden explícitamente. El objetivo de este Servicio es ayudar al Cliente a decidir el mejor procedimiento a seguir para las áreas de enfoque del PCI PIN y asistirlo al momento de determinar si es capaz de atravesar una evaluación de seguridad de PCI PIN y, cuando sea posible, de identificar las áreas de prioridad sugeridas para la corrección.

Fase III: elaboración de informes

El Servicio no incluye ningún informe final, solo se trata de un servicio de consultoría por hora.

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 y requisitos de recursos.
- Programar y llevar a cabo reuniones iniciales, periódicas de seguimiento y de cierre.
- Entrevistar al personal correspondiente de la organización y recopilar información al respecto.
- Proporcionar al Cliente comentarios sobre las observaciones identificadas durante el Servicio que podrían requerir corrección.

RESPONSABILIDADES 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 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 usa como referencia los requisitos y procedimientos de prueba del Estándar vigente aplicable al momento de la fecha de inicio del Servicio.
- El Servicio no incluye ningún informe final, solo se trata de un servicio de consultoría por hora.
- Los Servicios no incluyen pruebas o revisiones detalladas de los ajustes del sistema, configuraciones u observación de los procesos y procedimientos implementados.
- El Servicio no incluye visitas a terceros utilizados como respaldo para el entorno de PCI PIN del Cliente.
- El Servicio puede constar de actividades de evaluación remotas e in situ.
- 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.
- Todos los servicios de PCI PIN seleccionados para una única declaración de trabajo (Statement of Work, SOW) o Formulario de pedido deben prestarse durante el mismo plazo. 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 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.