AMERICAN EXPRESS

Política Operativa de Seguridad de los Datos

Sección 1 Introducción a la DSOP y Estándares de Protección 3

Sección 2 Programa de Cumplimiento de PCI DSS (Validación Periódica Importante de sus Sistemas) 3

Medida 1: Participar en el Programa de Cumplimiento de American Express de acuerdo con esta Política 4
Medida 2: Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento 4
Medida 3: Completar la Documentación de Validación que debe enviar a American Express 7
Medida 4: Enviar la Documentación de Validación a American Express 9

Sección 3 Obligaciones de administración de los Incidentes de Datos 10

Sección 4 Obligaciones de indemnización por un Incidente de Datos 12

Sección 5 Programa de Análisis Dirigido (TAP) 14

Sección 6 Confidencialidad 16

Sección 7 Exención de responsabilidad 16

Sección 8 Glosario 16

Sección 9 Sitios web útiles 20

AMERICAN EXPRESS

Resumen de cambios de la DSOP

Iconos

Las actualizaciones importantes se muestran en la Tabla de resumen de cambios y se indican también en la *DSOP* con una barra de cambio. Una barra de cambio es una línea vertical, normalmente en el margen izquierdo, que identifica el texto agregado o revisado. Solo los cambios sustanciales en la *DSOP* con posibles impactos en los procedimientos operativos de un Establecimiento se indican con una barra de cambio como se muestra en el margen izquierdo.

El texto eliminado se resalta con un icono de bote de basura colocado en el margen junto a una eliminación significativa de texto, incluidas secciones, tablas, párrafos, notas y viñetas. Se hace referencia al texto eliminado en este Resumen de cambios con la numeración de la sección de la publicación anterior para evitar confusiones.

Las líneas azules en los bordes de los párrafos indican información específica de la región.

Tabla de resumen de cambios

Las actualizaciones importantes se muestran en la siguiente tabla y se indican también en la *DSOP* con una barra de cambio.

Sección/Subsección	Descripción del cambio
No hay cambios en esta versión.	

Sección 1 Introducción a la DSOP y Estándares de Protección

Como líder en protección al consumidor, American Express siempre ha asumido el compromiso de proteger los Datos de los Tarjetahabientes y los Datos Confidenciales de Autenticación con el fin de garantizar que se mantengan seguros.

Si los datos se encuentran comprometidos, los consumidores, los Establecimientos, los Proveedores de Servicios y los emisores de tarjetas se ven afectados en igual medida. Basta un solo incidente para perjudicar gravemente la reputación de una empresa y su capacidad para hacer negocios de forma eficaz. Las acciones dirigidas a mitigar esa amenaza con la implementación de políticas operativas de seguridad pueden ayudar a mejorar la confianza del cliente, aumentar la rentabilidad y optimizar la reputación de una empresa.

American Express sabe que nuestros Establecimientos y Proveedores de Servicios (en conjunto, usted) comparten nuestra preocupación y, como parte de sus responsabilidades, requiere que **usted** cumpla con las disposiciones de seguridad de datos en su contrato para aceptar (en el caso de Establecimientos) o procesar (en el caso de los Proveedores de Servicios) la Tarjeta American Express® (cada uno, respectivamente, el **Contrato**) y esta Política Operativa de Seguridad de los Datos (DSOP), que podemos modificar cada cierto tiempo. Estos requisitos se aplican a todos sus equipos, sistemas y redes —incluidos sus componentes— en los que se almacenen, procesen o transmitan claves de Cifrado, Datos del Tarjetahabientes o Datos Confidenciales de Autenticación (o una combinación de estos).

Los términos en mayúscula utilizados que no se definen en el texto de este documento tienen el significado que se les atribuye en el glosario incluido al final de la presente política.

La Política Operativa de Seguridad de los Datos (DSOP) es un conjunto de requisitos integrales de políticas diseñados para proteger Datos de Cuenta siempre que dichos datos se almacenen, procesen o transmitan.

American Express requiere que todos los Establecimientos y Proveedores de Servicio cumplan con el Estándar de Seguridad de los Datos de la Industria de las Tarjetas de Pago (PCI DSS). Como parte de ese requisito, usted y sus partes cubiertas deben hacer lo siguiente:

- Guardar los Datos del Tarjetahabiente solo para facilitar las Transacciones con la Tarjeta American Express de conformidad con, y según lo requiere, el Contrato.
- Cumplir con la versión actual de los requisitos del PCI DSS y otros requisitos del Consejo de los Estándares de Seguridad de la PCI (PCI SCC) aplicables a su procesamiento, almacenamiento o transmisión de Claves de Cifrado, Datos del Tarjetahabiente o Datos de Autenticación Confidenciales; a más tardar en la fecha de vigencia para implementar esa versión del requisito aplicable.
- Asegurarse de que se utilicen los productos aprobados por la PCI al implementar o reemplazar la tecnología para almacenar, procesar o transmitir datos.

Usted debe proteger todos los Registros de Cargos de American Express, y los Registros de Crédito retenidos según el Contrato de acuerdo con estas disposiciones de seguridad de los datos; debe utilizar estos registros solo con fines del Contrato y protegerlos correspondientemente. Usted es responsable financieramente y de otro modo ante American Express de asegurar que sus Partes Cubiertas cumplan con estas disposiciones de seguridad de los datos (además de demostrar el cumplimiento de sus Partes Cubiertas con esta política bajo la Sección 2, "Programa de Cumplimiento de PCI DSS (Validación Periódica Importante de sus Sistemas)", excepto que se disponga lo contrario en esa sección). Los detalles respecto a los Estándares PCI y cómo cumplir con sus requisitos pueden verse en www.pcisecuritystandards.org.

Sección 2 Programa de Cumplimiento de PCI DSS (Validación Periódica Importante de sus Sistemas)

Usted debe tomar las medidas siguientes para validar bajo el PCI DSS anualmente y cada 90 días, como se describe a continuación, el estado de sus equipos, redes o sistemas (y sus componentes) y los de sus Franquiciatarios, en los cuales se almacenan, procesan o transmiten los Datos del Tarjetahabiente o Datos de Autenticación Confidenciales.

Las medidas necesarias para completar la validación son las cuatro siguientes:

- Medida 1: Participar en el programa de cumplimiento de PCI de American Express de acuerdo con esta política.
- Medida 2: Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento.
- Medida 3: Completar la Documentación de Validación que debe enviar a American Express.
- Medida 4: Enviar la Documentación de Validación a American Express dentro de los plazos establecidos.

Medida 1: Participar en el Programa de Cumplimiento de American Express de acuerdo con esta Política

Los Establecimientos de Nivel 1, Establecimientos de Nivel 2 y todos los Proveedores de Servicios, como se describe a continuación, deben participar en el Programa de acuerdo con esta política. American Express puede designar, a nuestro exclusivo criterio, a Establecimientos de Nivel 3 y de Nivel 4 específicos para participar en el Programa conforme a esta política.

Los Establecimientos y Proveedores de Servicios que deben participar en el Programa deben inscribirse en el Portal proporcionado por el administrador del Programa seleccionado por American Express dentro de los plazos establecidos.

- Debe aceptar todos los términos y condiciones razonables asociados con el uso del Portal.
- Debe asignar y proporcionar información precisa para al menos un contacto de seguridad de datos dentro del Portal. La información requerida incluye:
  - Nombre completo
  - Dirección de correo electrónico
  - Número de teléfono
  - Dirección física de envío
- Debe proporcionar información de contacto actualizada o nueva para el contacto de seguridad de datos asignado dentro del Portal cuando la información cambie.
- Debe asegurarse de que sus sistemas estén actualizados para permitir las comunicaciones de servicio desde el dominio designado del Portal.

Si usted deja de proporcionar o mantener actualizada la información de contacto de seguridad de datos o habilitar las comunicaciones por correo electrónico esto no afectará nuestros derechos a aplicar tarifas de no validación.

Medida 2: Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento

Existen cuatro niveles aplicables a los Establecimientos y dos niveles aplicables a los Proveedores de Servicios de acuerdo con su volumen de Transacciones con Tarjetas de American Express.

- Para los Establecimientos, este es el volumen presentado por sus Establecimientos que se acumulan hasta el nivel más alto de cuenta de Establecimiento de American Express.*
- Para los Proveedores de Servicios, esta es la suma del volumen presentado por el Proveedor de Servicios y las Entidades proveedoras de servicios a las que presta servicios.

Las Transacciones de pagos iniciados por el comprador (BIP) no están incluidas en el volumen de Transacciones con Tarjetas de American Express para determinar los requisitos de validación y el Nivel del Establecimiento. Usted recibirá una de las categorías de Nivel de Establecimiento especificadas en la Tabla A-1: Niveles de Establecimiento o Proveedor de Servicios.

* En el caso de los Franquiciantes, esto comprende el volumen de sus Establecimientos Franquiciatarios. Los Franquiciantes que exigen que sus Franquiciatarios utilicen un Sistema de punto de venta (POS) o Proveedor de Servicios especificado también deben proporcionar Documentación de Validación para los Franquiciatarios afectados.

Tabla A-1: Niveles de Establecimiento o Proveedor de Servicios

Nivel de Establecimiento	Transacciones anuales de American Express
Establecimiento de Nivel 1	procesa 2.5 millones de Transacciones de Tarjetas American Express o más por año, o cualquier Establecimiento al que American Express, a su criterio, le asigna el Nivel 1.
Establecimiento de Nivel 2	procesa de 50,000 a menos de 2.5 millones de Transacciones de Tarjetas American Express por año.
Establecimiento de Nivel 3	procesa de 10,000 a menos de 50,000 Transacciones de Tarjetas American Express por año.
Establecimiento de Nivel 4	procesa menos de 10,000 Transacciones de Tarjetas American Express por año.
Nivel de Proveedor de Servicios	**Transacciones anuales de American Express**
Proveedor de Servicios de Nivel 1	procesa 2.5 millones de Transacciones de Tarjetas American Express o más por año, o cualquier Proveedor de Servicios que American Express considere de otra manera como Nivel 1.
Proveedor de Servicios de Nivel 2	procesa menos de 2.5 millones de Transacciones de Tarjetas American Express por año, o cualquier Proveedor de Servicios que American Express no considere como Nivel 1.

Requisitos de la Documentación de Validación del Establecimiento

Los Establecimientos (no los Proveedores de Servicios) tienen cuatro posibles clasificaciones de Nivel de Establecimiento. Después de determinar el Nivel del Establecimiento a partir de la Tabla A-1: Niveles de Establecimiento o Proveedor de Servicios (arriba), consulte la Tabla A-2: Documentación de Validación del Establecimiento para determinar los requisitos de la documentación de validación.

Tabla A-2: Documentación de Validación del Establecimiento

Nivel del Establecimiento/ Transacciones anuales de American Express	Informe de Cumplimiento de la Certificación del Cumplimiento (ROC AOC)	Cuestionario de Autoevaluación de Certificación de Cumplimiento (SAQ AOC) Y Escaneo Trimestral Externo de Vulnerabilidad de la Red (Escaneo)	Certificación del Programa de mejora de tecnología de seguridad (STEP) para Establecimientos elegibles
Nivel 1/ 2.5 millones o más	Obligatorio	No corresponde	Opcional con aprobación de American Express (reemplaza al ROC)
Nivel 2/ 50,000 a menos de 2.5 millones	Opcional	SAQ AOC obligatorio (a menos que presente un ROC AOC); escaneo obligatorio con ciertos tipos de SAQ	Opcional con aprobación de American Express* (reemplaza al SAC y escaneo de red o ROC)
Nivel 3**/ 10,000 a menos de 50,000	Opcional	SAQ AOC opcional (obligatorio si lo exige American Express); escaneo obligatorio con ciertos tipos de SAQ	Opcional con aprobación de American Express* (reemplaza al SAQ y escaneo de red o ROC)
Nivel 4**/ Menos de 10,000	Opcional	SAQ AOC opcional (obligatorio si lo exige American Express); escaneo obligatorio con ciertos tipos de SAQ	Opcional con aprobación de American Express* (reemplaza al SAQ y escaneo de red o ROC)

* **Nota:** El equipo de American Express PCI revisará la solicitud y elegibilidad y confirmará si califica al Programa STEP. Comuníquese con su Gerente de Clientes y/o AXPPCIComplianceProgram@aexp.com para verificar la elegibilidad.

**Para evitar dudas, los Establecimientos de Nivel 3 y de Nivel 4 no deben presentar Documentación de Validación, a menos que American Express así lo exija a su exclusivo criterio; no obstante, deben cumplir con todas las demás disposiciones de esta Política Operativa de Seguridad de los Datos y quedan sujetos a ellas.

American Express se reserva el derecho de verificar la integridad, exactitud, y adecuación de la Documentación de Validación de su PCI. American Express puede solicitarle que proporcione documentos de respaldo adicionales para la evaluación en apoyo de este propósito. Además, American Express tiene derecho a solicitarle que contrate un Evaluador de Seguridad Calificado (QSA) o Investigador Forense PCI (PFI) aprobado por el PCI Security Standards Council.

Requisitos de Documentación de Validación de los Proveedores de Servicios

Los Proveedores de Servicios (no los Establecimientos) tienen dos posibles clasificaciones de Nivel. Después de determinar el Nivel del Proveedor de Servicio a partir de la Tabla A-1: Niveles de Establecimiento o Proveedor de Servicios (arriba), consulte la Tabla A-3: Documentación de Validación de los Proveedores de Servicios para determinar los requisitos de la documentación de validación.

Proveedores de Servicios que no son elegibles para STEP.

Tabla A-3: Documentación de Validación de los Proveedores de Servicios

Nivel	Documentación de validación	Requisito
1	Informe Anual de Cumplimiento de la Certificación del Cumplimiento (ROC AOC)	Obligatorio
2	SAQ D Anual (Proveedor de Servicios) y Escaneo de Red Trimestral o Informe Anual sobre el Cumplimiento de la Certificación del Cumplimiento (ROC AOC), si se prefiere	Obligatorio

Se recomienda que los Proveedores de Servicios también cumplan con los requisitos de validación complementaria de las entidades designadas por la PCI.

Programa de mejora de tecnología de seguridad (STEP)

Los Establecimientos que cumplen con el PCI DSS también pueden, de acuerdo con el criterio de American Express, reunir los requisitos del Programa de mejora de tecnología de seguridad (STEP) de American Express si implementan determinadas tecnologías de seguridad adicionales en sus entornos de procesamiento de Tarjetas. El STEP solo se aplica si el Establecimiento no ha tenido un Incidente de Datos durante los 12 meses anteriores y si el 75 % de sus Transacciones con Tarjeta se realiza mediante una combinación de las siguientes opciones de seguridad mejoradas:

- **EMV, EMV Contactless o Cartera Digital**: en un Dispositivo con Chip Activo que tenga una aprobación o certificación EMVCo (www.emvco.com) válida y vigente y que sea capaz de procesar las Transacciones de Tarjetas con Chip compatibles con la AEIPS (Especificación de Pago con Circuito Integrado de American Express). (Los Establecimientos de EE. UU. deben incluir Contactless)
- **Cifrado de Punto a Punto (P2PE)**: comunicación con el procesador del Establecimiento mediante un sistema de Cifrado de Punto a Punto aprobado por los PCI SSC o QSA
- **Tokenización**: la solución de uso del token implementada debe:
  - cumplir con las especificaciones de EMVCo,
  - estar protegida, procesada, almacenada, transmitida y administrada en su totalidad por un proveedor de servicios externo compatible con PCI, y
  - el Token no se puede revertir para revelar los Números de Cuenta Principal (PAN) no enmascarados al Establecimiento.

Los Establecimientos que pueden participar en el STEP tienen que cumplir menos requisitos de Documentación de Validación de la PCI, tal como se describe más adelante en la Medida 3: "Completar la Documentación de Validación que debe enviar a American Express" a continuación.

Medida 3: Completar la Documentación de Validación que debe enviar a American Express

Los siguientes documentos son necesarios para diferentes niveles de Establecimientos y Proveedores de Servicios como se enumeran en la Tabla A-2: Documentación de Validación del Establecimiento y en la Tabla A-3: Documentación de Validación de los Proveedores de Servicios anteriores.

Debe proporcionar la Certificación de cumplimiento (AOC) para el tipo de evaluación aplicable. El AOC es una declaración de su estado de cumplimiento y, como tal, debe estar firmado y fechado por el nivel de liderazgo apropiado dentro de su organización.

Además del AOC, American Express puede solicitarle que proporcione una copia de la evaluación completa y, a nuestro criterio, documentos de respaldo adicionales que demuestren el cumplimiento de los requisitos de PCI DSS. Esta Documentación de Validación corre por su cuenta.

Informe de Cumplimiento de la Certificación del Cumplimiento (ROC AOC) - (Requisito anual): El informe de Cumplimiento documenta los resultados de un examen detallado en el sitio de sus equipos, sistemas y redes (y sus componentes) en los que se almacenen, procesen o transmitan Datos del Tarjetahabiente o Datos Confidenciales de Autenticación (o una combinación de estos). Existen dos versiones: una para los Establecimientos y otra para los Proveedores de Servicios. El Informe de Cumplimiento debe ser realizado por:

- un QSA, o
- un Asesor de Seguridad Interna (ISA) y atestiguada por su director ejecutivo, su director de finanzas, su director de seguridad de la información o su director general

El ROC AOC debe estar firmado y fechado por un QSA o ISA y el nivel de liderazgo autorizado dentro de su organización y entregado a American Express al menos una vez al año.

Cuestionario de Autoevaluación de la Certificación del Cumplimiento (SAQ AOC) - (Requisito Anual): Los Cuestionarios de Autoevaluación permiten realizar una autoevaluación de sus equipos, sistemas y redes (y sus componentes) donde se almacenan, procesan o transmiten Datos del Tarjetahabiente o Datos de Autenticación Confidenciales (o ambos). Existen varias versiones del SAQ. Usted seleccionará una o más en función de su Entorno de Datos del Tarjetahabiente.

El SAQ puede ser completado por personal dentro de su Compañía calificado para responder las preguntas de manera precisa y completa o puede contratar a un QSA para que lo ayude. El SAQ AOC debe estar firmado y fechado por un QSA del nivel de liderazgo autorizado dentro de su organización y entregado a American Express al menos una vez al año.

Resumen de Escaneo Externo de Vulnerabilidad de Red por un Proveedor de Escaneo Aprobado (ASV Scan) - (Requisito de 90 días): Un escaneo externo de vulnerabilidad es una prueba remota para ayudar a identificar debilidades, vulnerabilidades potenciales y configuraciones incorrectas de los componentes de Internet de su Entorno de Datos del Tarjetahabiente (por ejemplo, sitios web, aplicaciones, servidores web, servidores de correo, dominios públicos o hosts).

El escaneo ASV debe llevarse a cabo por un Proveedor de Escaneo Aprobado (ASV).

Si lo requiere el SAQ, el Informe de Escaneo ASV y de Certificación de Cumplimiento de Escaneo (AOSC) o el resumen ejecutivo que incluye un recuento de los objetivos escaneados, la certificación de que los resultados cumplen con los procedimientos de escaneo del PCI DSS y el estado de cumplimiento completado por ASV, deben presentarse a American Express al menos una vez cada 90 días.

Si presenta un ROC AOC o STEP, usted no está obligado a proporcionar un resumen ejecutivo de AOSC o de Escaneo ASV a menos que esto se solicite específicamente. Con el objetivo de disipar dudas, los escaneos son obligatorios si así lo exige el SAQ aplicable.

Documentación de Validación de Certificación de STEP (STEP) - (Requisito anual): STEP solo está disponible para los Establecimientos que cumplen con los criterios enumerados en la Medida 2: "Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento" anterior. Si su empresa califica, debe completar y presentar anualmente el formulario de Certificación de STEP a American Express. El formulario de Certificación Anual STEP está disponible para su descarga desde el Portal. También puede comunicarse con su Gerente de Clientes o escribir a American Express al AXPPCIComplianceProgram@aexp.com.

Incumplimiento del PCI DSS - (Requisito anual, 90 días y/o ad hoc): Si no cumple con el PCI DSS, entonces debe presentar un Resumen de la Herramienta de Enfoque Priorizado (PAT) PCI (disponible para su descarga a través del sitio web de PCI Security Standards Council).

El Resumen PAT debe designar una fecha de corrección que no exceda un plazo de doce (12) meses a partir de la fecha de finalización del documento con el fin de lograr el cumplimiento. Usted debe proporcionar a American Express actualizaciones periódicas de su avance en la remediación del estado de incumplimiento (Establecimientos de Nivel 1, Nivel 2, Nivel 3 y Nivel 4; todos los Proveedores de Servicio). Las medidas de remediación necesarias para lograr el cumplimiento del PCI DSS corre por su cuenta.

American Express no impondrá tarifas de incumplimiento previo a la fecha de remediación. Conforme a la Tabla A-4: Tarifa de Incumplimiento, usted sigue siendo responsable ante American Express por todas las obligaciones de indemnización por un Incidente de Datos y está sujeto a todas las demás disposiciones de esta política.

American Express, a su exclusivo criterio, retiene el derecho de imponer tarifas de incumplimiento si:

- no se presentó una Plantilla de Enfoque Priorizado PCI conforme con los requisitos enunciados en esta sección,
- no se cumplieron los pasos de remediación delimitados en la Plantilla de Enfoque Priorizado PCI para Estados de Incumplimiento,
- no se cumplieron los requisitos de la Plantilla de Enfoque Priorizado PCI para Estados de Incumplimiento, o
- no se proporcionó la documentación obligatoria de cumplimiento a American Express antes de la fecha límite aplicable o ante la solicitud.

Los Establecimientos/Proveedores de Servicios que no cumplen con los requisitos detallados en la Medida 2: Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento, podría estar sujeto a tarifas conforme a lo enunciado en la Medida 4: Enviar la Documentación de Validación a American Express.

Con el objetivo de disipar toda duda, los Establecimientos que no cumplan con el PCI DSS no pueden participar en el STEP.

Medida 4: Enviar la Documentación de Validación a American Express

Todos los Establecimientos y Proveedores de Servicios que deben participar en el Programa deben presentar la Documentación de Validación marcada como "obligatoria" en las tablas de la Medida 2: "Comprender sus Requisitos de Documentación de Validación y de Nivel del Proveedor de Servicios/Establecimiento" de American Express antes de las fechas límites aplicables.

Debe presentar su Documentación de Validación a American Express utilizando el Portal provisto por el Administrador del Programa seleccionado por American Express. Al presentar la Documentación de Validación, usted declara y garantiza a American Express que lo siguiente es cierto (en la medida de sus posibilidades):

- Su evaluación fue completa y minuciosa;
- El estado del PCI DSS se representó con precisión al momento de completarlo, ya sea presentando la Certificación de Cumplimiento (AOC) o un Resumen de la Herramienta de Enfoque Priorizado (PAT) de PCI por incumplimiento;
- Usted está autorizado a divulgar la información contenida en el mismo y proporcionar la Documentación de Validación a American Express sin violar los derechos de ninguna otra parte.

Tarifas de Incumplimiento y Cancelación del Contrato

American Express tiene derecho a imponerle tarifas de incumplimiento y cancelar el Contrato si no cumple con estos requisitos o si no proporciona la documentación obligatoria de validación a American Express antes de la fecha límite aplicable. American Express intentará notificar al contacto de seguridad de datos acerca de la fecha límite aplicable para cada período de elaboración de informes anual y trimestral.

Tabla A-4: Tarifa de Incumplimiento

Descripción*	Establecimiento de Nivel 1 o Proveedor de Servicios de Nivel 1	Establecimiento de Nivel 2 o Proveedor de Servicios de Nivel 2	Establecimiento de Nivel 3 o Nivel 4
Se evaluará una tarifa de incumplimiento si la documentación de validación no se recibe en la primera fecha límite.	USD $25,000	USD $5,000	USD $50
Se evaluará una tarifa adicional de incumplimiento si la documentación de validación no se recibe en la segunda fecha límite.	USD $35,000	USD $10,000	USD $100
Se evaluará una tarifa adicional de incumplimiento si la documentación de validación no se recibe en la tercera fecha límite. **NOTA:** Las tarifas de incumplimiento se siguen aplicando hasta que se presente la documentación de cumplimiento.	USD $45,000	USD $15,000	USD $250

* Las Tarifas de Incumplimiento se evaluarán en equivalentes de la Divisa Local.

* No aplica en Argentina.

Si sus obligaciones de la documentación de cumplimiento del PCI DSS no se cumplen, American Express tiene el derecho de imponer las tarifas de incumplimiento de forma acumulativa, retener pagos y/o rescindir el Contrato.

Sección 3 Obligaciones de administración de los Incidentes de Datos

Debe notificar a American Express de inmediato y en ningún caso después de setenta y dos (72) horas de descubrir un Incidente de Datos.

Para notificar a American Express, comuníquese con el Programa de Respuesta a Incidentes Empresariales de American Express (*EIRP*) a la línea gratis 1.888.732.3750, o al 1.602.537.3021, o por correo electrónico a EIRP@aexp.com. Debe nombrar a una persona como su contacto en relación con ese Incidente de Datos. Además:

- Debe conducir una investigación minuciosa de cada Incidente de Datos y proporcionar de inmediato a American Express todos los Números de Tarjeta Comprometidos. American Express se reserva el derecho de llevar a cabo su propio análisis interno para identificar los Números de Tarjetas involucrados en el Incidente de Datos.

Para Incidentes de Datos que involucren menos de 10,000 Números de Tarjeta únicos, se debe proporcionar un resumen de investigación a American Express dentro de los diez (10) días hábiles de su finalización.

- Los resúmenes de investigación deben tener la información siguiente: resumen del incidente, descripción de los ambientes afectados, cronología de los eventos, fechas clave, detalles de exposición de datos e impacto, acciones de contención y remediación, y certificación de que no hay indicios de datos adicionales de American Express en riesgo.

Para los Incidentes de Datos que impliquen 10,000 o más Números de Tarjeta únicos, debe contratar a un PFI de la PCI para llevar a cabo esta investigación en un plazo de cinco (5) días después del descubrimiento de un Incidente de Datos.

- Se le debe proporcionar el informe de la investigación forense sin editar a American Express en un plazo de diez (10) días hábiles después de su finalización.
- Los informes de investigación forense se deben completar con la Plantilla del Informe Forense Final del Incidente vigente disponible en la PCI. El informe debe incluir revisiones forenses, informes de cumplimiento y toda información relacionada con el Incidente de Datos; identificar la causa del Incidente de Datos; confirmar si usted cumplía o no con el PCI DSS en el momento del Incidente de Datos; y verificar su capacidad para prevenir futuros Incidentes de Datos (i) proporcionando un plan para remediar todas las deficiencias del PCI DSS y (ii) participando en el programa de cumplimiento de American Express (según se describe más abajo). Al solicitarlo American Express, usted debe proporcionar validación mediante un Asesor de seguridad calificado (QSA) de que las deficiencias se han remediado.

Sin perjuicio de los párrafos anteriores de esta Sección 3, "Obligaciones de administración de los Incidentes de Datos":

- American Express puede, a su exclusivo criterio, pedirle que contrate a un PFI para que lleve a cabo una investigación sobre un Incidente de Datos para los Incidentes de Datos que impliquen menos de 10,000 Números de Tarjetas únicos o donde han sucedido múltiples incidentes en un período de 12 meses. Toda investigación debe cumplir con los requisitos establecidos anteriormente en esta Sección 3, "Obligaciones de administración de los Incidentes de Datos" y debe finalizarse dentro del marco de tiempo requerido por American Express.
- American Express puede, a su exclusivo criterio, contratar por separado a un PFI para llevar a cabo una investigación sobre cualquier Incidente de Datos y puede cobrarle a usted el costo de dicha investigación.

Debe evaluar el Incidente de Datos conforme a las leyes aplicables globales de notificación ante violación de datos y, cuando se considere necesario, notificar a los reguladores aplicables y a los Tarjetahabientes afectados conforme a dichas lees de notificación ante violación de datos. Si ha determinado que su Proveedor de Servicios u otra entidad es responsable de informar el Incidente de Datos, debe avisar a dicho Proveedor de Servicios o entidad de su deber de evaluar sus obligaciones de reportar conforme a las leyes aplicables de notificación ante violación de datos. Acepta obtener aprobación escrita de American Express antes de hacer referencia o nombrar a American Express en cualquier comunicación a los Tarjetahabientes sobre el incidente de datos. Usted acepta trabajar con American Express para proporcionar detalles y rectificar cualquier problema que se derive del Incidente de Datos, incluyendo proporcionar (y obtener cualquier exención de responsabilidad que sea necesario proporcionar) a American Express toda la información relevante para verificar su capacidad de prevenir Incidentes de Datos futuros de una manera consistente con el Contrato.

Sin perjuicio de cualquier obligación de confidencialidad que disponga lo contrario en el Contrato, American Express tiene el derecho de divulgar información sobre cualquier Incidente de Datos a los Tarjetahabientes, los Emisores, otros participantes en la Red de American Express y al público en general, si la Ley Aplicable así lo exige; en virtud de una resolución, sentencia, orden o solicitud judicial, administrativa o regulatoria u otro proceso; con el fin de mitigar el riesgo de fraude u otros daños; o de cualquier forma que sea apropiada para operar la Red de American Express.

¿Qué debe hacerse en el caso de que ocurra un Incidente de Datos?

Siga los siguientes pasos si ha identificado un Incidente de Datos en su negocio.

Paso 1:

Complete el Formulario de Aviso Inicial de Incidente de Datos del Establecimiento y envíelo por correo electrónico a EIRP@aexp.com en el transcurso de las 72 horas posteriores al descubrimiento del Incidente de Datos.

Paso 2:

Realice una investigación exhaustiva; esto puede requerir que contrate a un Investigador forense de la Industria de las Tarjetas de Pago (PCI).

Paso 3:

Facilítenos inmediatamente todos los Números comprometidos de las Tarjetas American Express®.

Paso 4:

Trabaje con nosotros para ayudar a resolver los problemas derivados del Incidente de Datos.

Ver la Sección 3, "Obligaciones de administración de los Incidentes de Datos" para obtener más detalles sobre las Obligaciones de administración de los Incidentes de Datos.

¿Tiene alguna pregunta?

EE. UU.: (888) 732-3750 (llamada gratuita)

Internacional: +1 (602) 537-3021

EIRP@aexp.com

Sección 4 Obligaciones de indemnización por un Incidente de Datos

Sus obligaciones de indemnización con American Express bajo el Contrato por los Incidentes de Datos se determinarán, sin renunciar a ninguno de los demás derechos y compensaciones de American Express, en esta Sección 4, "Obligaciones de indemnización por un Incidente de Datos". Además de sus obligaciones de indemnización (de haberlas), usted puede estar sujeto a una tarifa de incumplimiento de Incidente de Datos como se describe a continuación en la Sección 4, "Obligaciones de indemnización por un Incidente de Datos".

Debe compensar a American Express una tarifa de $5 USD por cada número de cuenta, por Incidentes de Datos que involucren:

- 10,000 o más Números de Tarjetas de American Express con cualquiera de lo siguiente:
  - Datos de Autenticación Confidenciales, o
  - Fecha de Vencimiento

Sin embargo, American Express no pedirá una indemnización por un Incidente de Datos que implique lo siguiente:

- menos de 10,000 Números de Tarjetas de American Express, o
- más de 10,000 Números de Tarjetas de American Express, si usted cumple con las siguientes condiciones:
  - usted notificó a American Express sobre el Incidente de Datos de conformidad con la Sección 3, "Obligaciones de administración de los Incidentes de Datos",
  - usted estaba en cumplimiento en el momento del Incidente de Datos con el PCI DSS (según lo determina la investigación del PFI sobre el Incidente de Datos), y

- el Incidente de Datos no fue ocasionado por su conducta ilegítima ni la de sus Partes Cubiertas.

No obstante los párrafos anteriores de esta Sección 4, "Obligaciones de indemnización por un Incidente de Datos", para cualquier Incidente de Datos, sin importar la cantidad de Números de Tarjetas American Express, usted deberá pagar a American Express una cuota por incumplimiento de Incidente de Datos que no sea mayor a $100,000 USD por cada Incidente de Datos (según lo determine American Express a su exclusivo criterio) en el caso de que usted no cumpla con cualquiera de sus obligaciones establecidas en la Sección 3, "Obligaciones de administración de los Incidentes de Datos". Para evitar dudas, la tarifa total por incumplimiento de Incidentes de Datos evaluada para cualquier Incidente de Datos individual no deberá ser mayor a $100,000 USD.

American Express excluirá de su cálculo cualquier Número de Cuenta de Tarjeta American Express que haya estado implicado en una reclamación de indemnización por Incidente de Datos anterior realizada dentro de los doce (12) meses anteriores a la Fecha de Notificación. Todos los cálculos realizados por American Express conforme a esta metodología son definitivos.

American Express puede cobrarle el monto total de sus obligaciones de indemnización por Incidentes de Datos o deducir el monto de los pagos que American Express le hace (o lo cargará a su Cuenta Bancaria según corresponda) de conformidad con el Contrato.

Sus obligaciones de indemnización por los Incidentes de Datos mencionados aquí no se considerarán daños incidentales, especulativos, derivados, punitivos o ejemplares bajo el Contrato, siempre que dichas obligaciones no incluyan daños relacionados con ganancias o ingresos perdidos, pérdida de buena fe o pérdida de oportunidades de negocios, o daños de esta índole.

A su exclusivo criterio, American Express puede reducir la obligación de indemnización de los Establecimientos únicamente para los Incidentes de Datos que cumplan con cada uno de los siguientes criterios:

- Que la Tecnología para mitigar riesgos se haya utilizado con anterioridad al Incidente de Datos y que haya estado en uso durante la ventana de evento del Incidente de Datos,
- Que se haya llevado a cabo una investigación minuciosa según el programa PFI (a menos que algo diferente se haya acordado por escrito anteriormente),
- Que el informe forense especifique de manera clara la tecnología utilizada para mitigar riesgos en el procesamiento, almacenamiento, y/o transmisión de datos en el momento del Incidente de Datos, y
- Usted no almacena (ni ha almacenado durante toda la ventana de evento del Incidente de Datos) Datos de Autenticación Confidenciales ni ningún otro dato del Tarjetahabiente que no se haya vuelto ilegible.

Donde esté disponible una reducción de la indemnización, la reducción a su obligación de indemnización (sin incluir las tarifas de incumplimiento por pagar) se determina de la siguiente manera:

Tabla A-5: Criterios de reducción de la obligación de indemnización

Reducción de la obligación de indemnización	Criterios requeridos
Reducción estándar: 50 %	Que >75 % del total de las Transacciones se hayan procesado en Dispositivos habilitados con Chip[1] O
	Que la Tecnología para mitigar riesgos se haya utilizado en >75 % de las localidades del Establecimiento[2]
Reducción superior: 75 % a 100 %	Que >75 % del total de las Transacciones se hayan procesado en Dispositivos habilitados con Chip[1] Y que otra tecnología para mitigar riesgos se haya implementado en >75 % de las localidades del Establecimiento[2]

[1] Según lo determine el análisis interno de American Express

[2] Según lo determine la investigación del PFI

- La reducción superior (del 75 % al 100 %) se determinará a partir del porcentaje más bajo entre el porcentaje de las Transacciones procesadas en Dispositivos habilitados con Chip Y el porcentaje de las localidades del Establecimiento que emplean otra Tecnología para mitigar riesgos. Los ejemplos en la Tabla A-6: Reducción de la obligación de indemnización mejorada representan el cálculo de la reducción de la indemnización.
- Para calificar como que usa una Tecnología para mitigar riesgos, usted deberá demostrar que esta se utiliza de manera efectiva de acuerdo con su diseño y propósito previsto.
- El porcentaje de las localidades que utilizan una Tecnología para mitigar riesgos es determinado por la investigación del PFI.
- La reducción de la obligación de indemnización no se aplica a las tarifas de incumplimiento que deban pagarse en relación con el Incidente de Datos.

Tabla A-6: Reducción de la obligación de indemnización mejorada

Ej.	Tecnologías para mitigar riesgos en uso	Elegible	Reducción
1	• El 80 % de las Transacciones se procesan en Dispositivos habilitados con Chip • El 0 % de las localidades emplea otra Tecnología para mitigar riesgos	No	50 %: Reducción Estándar (el porcentaje de uso de la Tecnología para mitigar riesgos es inferior al 75 %, por lo que no califica para recibir una Reducción Superior)[1]
2	• El 80 % de las Transacciones se procesan en Dispositivos habilitados con Chip • El 77 % de las localidades emplea otra Tecnología para mitigar riesgos	Sí	77 %: Reducción superior (el porcentaje de uso de la Tecnología para mitigar riesgos es del 77 %)
3	• El 93 % de las Transacciones se procesan en Dispositivos habilitados con Chip • El 100 % de las localidades emplea otra Tecnología para mitigar riesgos	Sí	93 %: Reducción superior (debido a que el 93 % de las Transacciones se procesan en Dispositivos habilitados con Chip)
4	• El 40 % de las Transacciones se procesan en Dispositivos habilitados con Chip • El 90 % de las localidades emplea otra Tecnología para mitigar riesgos	No	50 %: Reducción Estándar: (menos del 75 % de las Transacciones procesadas en Dispositivos habilitados con Chip, por lo que no califica para recibir una reducción superior)

[1] Un Incidente de Datos que implique 10,000 Cuentas de Tarjetas de American Express, a una tarifa de $5.00 USD por número de cuenta (10,000 x $5 = $50,000 USD) puede ser elegible para una reducción del 50 %, reduciendo las obligaciones de indemnización de $50,000 USD a $25,000 USD, sin incluir las tarifas de incumplimiento.

Sección 5 Programa de Análisis Dirigido (TAP)

Los Datos del Tarjetahabiente Comprometidos pueden deberse a brechas en la seguridad de los datos en su Entorno de Datos del Tarjetahabiente (CDE).

Los ejemplos de Datos del Tarjetahabiente comprometidos incluyen, entre otros:

- **Punto Común de Compra (CPP):** Los Tarjetahabientes de American Express informan Transacciones fraudulentas en las cuentas de su Tarjeta y estas se identifican y determinan que se han originado al realizar compras en sus Establecimientos.
- **Datos de la Tarjeta encontrados:** Los Datos de la Tarjeta y del Tarjetahabiente de American Express se encuentran en la red mundial vinculados a Transacciones en sus Establecimientos.
- **Sospecha de malware:** American Express sospecha que está utilizando un software infectado o vulnerable a códigos maliciosos.

El TAP está diseñado para identificar posibles Datos del Tarjetahabiente comprometidos.

Usted está obligado a cumplir, y debe hacer que sus Partes Cubiertas cumplan, con los siguientes requisitos tras la notificación de American Express de la posibilidad de que los Datos del Tarjetahabiente estén comprometidos.

- Debe revisar su CDE de inmediato para detectar las brechas en la seguridad de los datos y corregir todas las que encuentre.
  - Debe hacer que sus proveedores de servicios realicen una investigación exhaustiva de su CDE si han sido subcontratados.
- Debe proporcionar un resumen de las medidas tomadas o planificadas después de su revisión, evaluación y/o esfuerzos de corrección al recibir la notificación de American Express.
- Debe proporcionar documentos de validación del PCI DSS actualizados de acuerdo con la Sección 2, "Programa de Cumplimiento de PCI DSS (Validación Periódica Importante de sus Sistemas)".
- Según corresponda, usted debe contratar a un PFI de la PCI calificado para que examine su CDE en caso de que usted o su Parte Cubierta:
  - No pueda resolver los Datos del Tarjetahabiente Comprometidos dentro de un período de tiempo razonable, según lo determine American Express, o
  - Confirmar que ha ocurrido un Incidente de Datos y cumpla con los requisitos establecidos en la Sección 3, "Obligaciones de administración de los Incidentes de Datos".

Tabla A-7: Tarifa de incumplimiento del TAP

Descripción	Establecimiento de Nivel 1 o Proveedor de Servicios de Nivel 1	Establecimiento de Nivel 2 o Proveedor de Servicios de Nivel 2	Establecimiento de Nivel 3 o Nivel 4
Se podría aplicar una tarifa de incumplimiento cuando no se cumplen las obligaciones del TAP en la primera fecha límite.	USD $25,000	USD $5,000	USD $1,000
Se podría aplicar una tarifa de incumplimiento cuando no se cumplen las obligaciones del TAP en la segunda fecha límite.	USD $35,000	USD $10,000	USD $2,500
Se podría aplicar una tarifa de incumplimiento cuando no se cumplen las obligaciones del TAP en la tercera fecha límite. **NOTA:** *Las tarifas de incumplimiento pueden continuar aplicándose hasta que se cumplan las obligaciones o se resuelva el TAP.*	USD $45,000	USD $15,000	USD $5,000

Si sus obligaciones de TAP no se cumplen, American Express tiene el derecho de imponer las tarifas de incumplimiento de forma acumulativa, retener pagos y/o rescindir el Contrato.

Sección 6 Confidencialidad

American Express deberá tomar medidas razonables para mantener (y hacer que sus agentes y subcontratistas, incluyendo el proveedor del Portal, mantengan) sus informes sobre cumplimiento, incluyendo la Documentación de Validación confidencialmente y no divulgar la Documentación de Validación a un tercero (aparte de los Filiales, agentes, representantes, Proveedores de Servicios y subcontratistas de American Express) por un período de tres años a partir de la fecha de recepción, excepto que su obligación de confidencialidad no aplique a la Documentación de Validación que:

a. ya es del conocimiento de American Express antes de la divulgación;

b. es o se vuelve disponible para el público a través del incumplimiento de este párrafo por parte de American Express;

c. American Express reciba legítimamente de un tercero sin un deber de confidencialidad;

d. es desarrollado independientemente por American Express; o

e. se requiere que se divulgue mediante una orden del tribunal, dependencia administrativa o autoridad gubernamental, o por cualquier ley, regla o regulación o mediante una orden judicial, petición de descubrimiento, citación u otro proceso administrativo o legal, o por cualquier consulta formal o informal o investigación por cualquier dependencia o autoridad gubernamental (incluyendo cualquier entidad reguladora, inspector, examinador o dependencia del orden público).

Sección 7 Exención de responsabilidad

AMERICAN EXPRESS POR ESTE MEDIO RENUNCIA A TODAS LAS REPRESENTACIONES, GARANTÍAS Y RESPONSABILIDADES RESPECTO A ESTA POLÍTICA OPERATIVA DE SEGURIDAD DE LOS DATOS, PCI DSS, LAS ESPECIFICACIONES DE EMV Y LA DESIGNACIÓN Y DESEMPEÑO DE QSA, ASV O PFI (O CUALQUIERA DE ELLOS), YA SEA EXPRESA, IMPLÍCITA, LEGAL O DE OTRA MANERA, INCLUYENDO CUALQUIER GARANTÍA DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO ESPECÍFICO. LOS EMISORES DE LA TARJETA AMERICAN EXPRESS NO SON BENEFICIARIOS DE TERCEROS BAJO ESTA POLÍTICA.

Sección 8 Glosario

Para fines únicamente de esta *Resumen de cambios de la DSOP* las siguientes definiciones aplican y prevalecen en el caso de un conflicto con los términos que se encuentran en el *Reglamento para Establecimientos*:

Aplicación de Pago tiene el significado que se le da en el Glosario de términos actual para el Estándar de Software Seguro y el Estándar de Ciclo de Vida de Software Seguro, que está disponible en www.pcisecuritystandards.org.

Aprobado por la PCI significa que un Dispositivo de entrada del PIN o una Aplicación de pago (o ambos) aparece en el momento de desplegar la lista de compañías y proveedores aprobados mantenida por el PCI Security Standards Council, LLC, que está disponible en www.pcisecuritystandards.org.

Cargo significa un pago o compra hecha con la Tarjeta.

Certificación de cumplimiento (AOC) significa una declaración del estado de su cumplimiento con el PCI DSS, en la forma que lo indica el Payment Card Industry Security Standards Council, LLC.

Certificación de cumplimiento de escaneo (AOSC) significa una declaración del estado de su cumplimiento con los PCI DSS basada en un escaneo de la red, en la forma que lo indica el Payment Card Industry Security Standards Council, LLC.

Chip significa un microchip incrustado en una Tarjeta que contiene la información del Tarjetahabiente y de la cuenta.

Cifrado de Punto a Punto (P2PE) significa una solución que protege criptográficamente los datos de la cuenta desde el punto donde un Establecimiento acepta la tarjeta de pago hasta el punto seguro de descifrado.

Clave de Cifrado (clave de cifrado de American Express) significa todas las claves utilizadas en el procesamiento, generación, carga y/o protección de los datos de la cuenta. Esto incluye, entre otros, las siguientes:

- Claves de cifrado de clave: Claves maestras de zona (ZMK) y claves PIN de la zona (ZPK)
- Claves maestras que se usan en dispositivos criptográficos seguros: Claves maestras locales (LMK)
- Claves de código de seguridad de tarjeta (CSCK)
- Claves de PIN: Claves de derivación base (BDK), clave de cifrado de PIN (PEK) y ZPK

Consumidor es un tarjetahabiente que compra bienes, servicios o ambos.

Contrato se refiere a las Disposiciones Generales, el Reglamento para Establecimientos y todos los programas y anexos adjuntos, en conjunto (a veces denominado Contrato de Aceptación de la Tarjeta en nuestros materiales).

Crédito significa el monto del Cargo que usted reembolsa a los Tarjetahabientes por compras o pagos hechos con la Tarjeta.

Cuestionario de autoevaluación (SAQ) significa una herramienta de auto evaluación creada por el Payment Card Industry Security Standards Council, LLC, diseñada para evaluar y certificar el cumplimiento con el PCI DSS.

Datos de Autenticación Confidenciales significa información relacionada con la seguridad que se utiliza para autenticar tarjetahabientes y/o autorizar transacciones de tarjeta de pago. Esta información incluye, entre otros, códigos de verificación de la tarjeta, datos completos de la pista (de la banda magnética o equivalente en un chip), PIN y bloques de PIN.

Datos de Cuenta son los Datos del Tarjetahabiente y/o los datos de autenticación confidenciales. Consulte Datos del Tarjetahabiente y Datos de Autenticación Confidenciales.

Datos del Tarjetahabiente significa como mínimo, el Número de Cuenta Primario (PAN) completo por sí solo o el PAN completo más cualquiera de los siguientes: nombre del tarjetahabiente, fecha de vencimiento y/o código de servicio. Consulte los Datos de Autenticación Confidenciales para ver elementos de datos adicionales que puedan transmitirse o procesarse (pero no almacenarse) como parte de una transacción de pago.

Datos de Transacción significa toda la información requerida por American Express, que prueba una o más Transacciones, incluida la información obtenida en el punto de venta, información obtenida o generada durante la Autorización y la Presentación, y cualquier Contracargo.

Dispositivo de entrada del PIN tiene el significado que se le da en el Glosario de términos actual para el Punto de interacción (POI) de la Seguridad de la transacción del PIN (PTS) de la industria de Tarjetas de pago, los Requisitos de seguridad modular, que están disponibles en www.pcisecuritystandards.org.

Dispositivo Habilitado con Chip significa un dispositivo del punto de ventas que tiene una certificación/aprobación de EMVCo (www.emvco.com) y tiene la capacidad de procesar Transacciones de Tarjetas con Chip que cumplen con AEIPS.

Documentación de Validación significa la AOC que se presenta en relación con la Evaluación anual de seguridad en el sitio o SAQ, la AOSC y los resúmenes ejecutivos de hallazgos presentados en relación con los Escaneos de red trimestrales o la Certificación anual del programa de mejora de tecnología de seguridad.

Emisor de tarjeta significa cualquier Entidad (incluida American Express y sus filiales) con licencia de American Express o una filial de American Express para emitir Tarjetas y participar en el negocio de emisión de Tarjetas.

Entorno de Datos del Tarjetahabiente (CDE) significa las personas, los procesos y la tecnología que almacenan, procesan o transmiten datos del Tarjetahabiente o datos de autenticación confidenciales.

Especificaciones de la EMV significa las especificaciones emitidas por EMVCo, LLC, que están disponibles en www.emvco.com.

Establecimiento significa el Establecimiento y todas sus filiales que aceptan Tarjetas de American Express según un Contrato con American Express o sus filiales.

Establecimiento de nivel 1 significa un Establecimiento que procesa 2.5 millones de Transacciones de Tarjetas de American Express o más por año, o cualquier Establecimiento que American Express considere de nivel 1 por otro motivo.

Establecimientos de nivel 2 significa un Establecimiento que procesa de 50,000 a menos de 2.5 millones de Transacciones de Tarjetas de American Express al año.

Establecimiento de nivel 3 significa un Establecimiento que procesa de 10,000 a menos de 50,000 Transacciones de Tarjetas de American Express al año.

Establecimiento de nivel 4 significa un Establecimiento que procesa menos de 10,000 Transacciones de Tarjetas de American Express al año.

Estándar de seguridad de los datos de la industria de las Tarjetas de pago (PCI DSS) significa el Estándar de seguridad de los datos de la industria de las Tarjetas de pago que está disponible en www.pcisecuritystandards.org.

Evaluador de seguridad calificado (QSA) significa una entidad que ha sido clasificada por el Payment Card Industry Security Standards Council, LLC para validar el cumplimiento con el PCI DSS.

Fecha de Notificación significa la fecha en que American Express envía a los emisores la notificación final de un Incidente de Datos. Esta fecha depende de la fecha en que American Express recibe el informe forense final o el análisis interno y se determina al exclusivo criterio de American Express.

Franquiciatante es el operador de un negocio que autoriza a personas o Entidades (Franquiciatarios) a distribuir bienes o servicios u operar mediante la Marca del operador; brinda asistencia a los Franquiciatarios en la operación de sus negocios o influye en el método de operación del Franquiciatario; y requiere el pago de una cuota por los Franquiciatarios.

Franquiciatario significa un tercero de propiedad y operación independiente (incluidos licenciatarios, franquiciatarios o sucursales), que no es una Filial, que está licenciado por un Franquiciatante para operar una franquicia y que formalizó un contratos escrito con el Franquiciatante por medio del cual muestra de manera coherente la identificación externa que lo identifica de forma visible con la Marca del Franquiciatante o que se ofrece al público como un miembro del grupo de compañías de este.

Incidente de Datos significa un incidente que involucra la puesta en peligro o la presunta puesta en peligro de las Claves de Cifrado de American Express o, al menos, un número de Cuenta de Tarjeta American Express en que hay lo siguiente:

- un acceso o uso no autorizado de Claves de Cifrado, Datos del Tarjetahabiente o Datos de Autenticación Confidenciales (o una combinación de cada uno) que se almacenan, procesan o transmiten en sus equipos, sistemas o redes (o los componentes de estos) o el uso de los cuales usted exija o proporcione o haga disponible;
- el uso de dichas Claves de Cifrado, Datos del Tarjetahabiente o Datos de Autenticación Confidenciales (o una combinación de cada uno) que no sea el uso permitido por el Contrato; y/o
- la sospecha de una pérdida, robo o apropiación indebida por cualquier medio de materiales, registros o información que contienen dichas Claves de Cifrado, Datos del Tarjetahabiente o Datos de Autenticación Confidenciales (o una combinación de cada uno).

Información del Tarjetahabiente significa la información acerca de las Transacciones de la Tarjeta y los Tarjetahabientes de American Express, incluyendo nombres, direcciones, números de cuenta de tarjetas y números de identificación de las tarjetas (CID).

Investigador Forense de la PCI (PFI) significa una entidad que ha sido aprobada por el Payment Card Industry Security Standards Council, LLC para realizar investigaciones forenses de un incumplimiento o compromiso de los Datos de la Tarjeta de pago.

Nivel del Establecimiento significa la designación que asignamos a los Establecimientos en relación con sus obligaciones de validación de cumplimiento de PCI DSS, como se describe en la Sección 2, "Programa de Cumplimiento de PCI DSS (Validación Periódica Importante de sus Sistemas)".

Número de Cuenta Principal (PAN) tiene el significado que se le da en el glosario de términos actual del PCI DSS.

Número de Tarjeta significa el número de identificación único que el emisor asigna a la Tarjeta cuando la emite.

Número de Tarjeta Comprometido significa un número de Cuenta de Tarjeta American Express relacionado con un Incidente de Datos.

Partes Cubiertas significa todos sus empleados, agentes, representantes, subcontratistas, Procesadores, Proveedores de Servicio, proveedores de sus equipos de punto de venta (POS) o sistemas o soluciones de procesamiento de pago, Entidades asociadas con su cuenta de Establecimiento de American Express y cualquier otra parte a quien puede proporcionar acceso a los Datos de Autenticación Sensibles o Datos del Tarjetahabiente (o ambos) de conformidad con el Contrato.

PCI DSS significa el Estándar de seguridad de los datos de la industria de las Tarjetas de pago que está disponible en www.pcisecuritystandards.org.

Plantilla del Informe Forense Final del Incidente significa que la plantilla está disponible en el Consejo de Estándares de Seguridad de la PCI en www.pcisecuritystandards.org.

Portal, El significa el sistema de informes proporcionado por el administrador del Programa PCI de American Express seleccionado por American Express. Los Establecimientos y los Proveedores de Servicios deben utilizar El Portal para enviar la documentación de validación de PCI a American Express.

Procesador significa un Proveedor de Servicios de los Establecimientos que facilita el procesamiento de autorización y presentación a la red de American Express.

Programa de Análisis Dirigido (TAP) significa un programa que proporciona una identificación temprana de una posibilidad de que los Datos del Tarjetahabiente estén comprometidos en su Entorno de Datos del Tarjetahabiente (CDE). Consulte la Sección 5, "Programa de Análisis Dirigido (TAP)".

Programa de mejora de tecnología de seguridad (STEP) es el programa de American Express en el cual se alienta a los Establecimientos a implementar tecnologías que mejoran la seguridad de los datos.

Programa, El significa el Programa de Cumplimiento del PCI de American Express.

Proveedor de escaneo aprobado (ASV) significa una Entidad que ha sido calificada por el Payment Card Industry Security Standards Council, LLC para validar el cumplimiento con ciertos requisitos del PCI DSS al realizar escaneos de vulnerabilidad de los entornos de Internet.

Proveedor de Servicios de nivel 1 significa un Proveedor de Servicios que procesa 2.5 millones de Transacciones de Tarjetas de American Express o más al año, o cualquier Proveedor de Servicios que American Express considere como un nivel 1.

Proveedor de Servicios de nivel 2 significa un Proveedor de Servicios que procesa menos de 2.5 millones de Transacciones de Tarjetas de American Express al año, o cualquier Proveedor de Servicios que American Express no considere como nivel 1.

Proveedores de Servicios significa los procesadores autorizados, procesadores de terceros, proveedores de pasarela de pagos, integradores de Sistemas de POS y cualquier otro proveedor a los Establecimientos de Sistemas de POS u otras soluciones o servicios de procesamiento de pago.

Registro de Cargo significa un registro reproducible (impreso y electrónico) de un Cargo que cumple con nuestros requisitos y contiene el Número de Tarjeta, fecha de la Transacción, monto en dólares, Aprobación, firma del Tarjetahabiente (si corresponde) y otra información.

Registro de Crédito significa un registro de Crédito que cumple con nuestros requisitos.

Requisitos de seguridad del PIN de la PCI significa los requisitos de seguridad de los PIN de la industria de las Tarjetas de pago que están disponibles en www.pcisecuritystandards.org.

Requisitos del Payment Card Industry Security Standards Council (Consejo de los estándares de seguridad de la industria de las tarjetas de pago, PCI SCC) significa el conjunto de estándares y requisitos relacionados con la seguridad y protección de los datos de las tarjetas de pago, incluyendo el PCI DSS y PA DSS que están disponibles en www.pcisecuritystandards.org.

Sistema de punto de venta (POS) significa un sistema o equipos de procesamiento de información, incluyendo un terminal, computadora personal, caja registradora electrónica, lector Contactless o proceso o motor de pago, utilizado por un Establecimiento para obtener autorización o recolectar datos de la Transacción, o ambos.

Solución de Cifrado de Punto a Punto (P2PE), incluida en la lista de soluciones validadas de los PCI SSC, o validada por una compañía de P2PE de asesores de seguridad calificados de los PCI SSC.

Tarjeta American Express o **Tarjeta** significa cualquier tarjeta, dispositivo de acceso a la cuenta o servicio o dispositivo de pago con el nombre de American Express o con el nombre de una filial, logotipo, marca comercial, marca de servicio, nombre comercial u otro diseño o designación patentados y emitidos por un emisor o un número de Cuenta de tarjeta.

Tarjeta con Chip significa una Tarjeta que contiene un Chip y puede requerir un PIN como medio para verificar la identidad del Tarjetahabiente o la información de la cuenta incluida en el chip, o ambos (en nuestros materiales algunas veces se le denomina como "tarjeta inteligente", "Tarjeta EMV", "ICC" o "tarjeta de circuito integrado").

Tarjetahabiente significa una persona o entidad (i) que ha formalizado un contrato estableciendo una cuenta de tarjeta con un emisor o (ii) cuyo nombre aparece en la Tarjeta.

Tarjetahabiente significa un cliente al cual se le emite la tarjeta de pago o cualquier persona autorizada a usar la tarjeta de pago.

Tecnología para mitigar riesgos significa las soluciones tecnológicas que mejoran la seguridad de los Datos del Tarjetahabiente de American Express y los Datos de Autenticación Confidenciales, según lo determinado por American Express. A fin de que una tecnología para mitigar riesgos sea considerada como tal, deberá demostrar que esta se utiliza de manera efectiva de acuerdo con su diseño y propósito previsto. Los ejemplos incluyen, entre otros, lo siguiente: EMV, Cifrado de Punto a Punto y el uso de los token.

Token significa el token criptográfico que reemplaza al PAN, basado en un índice dado para un valor impredecible.

Transacción significa un Cargo, Crédito, Adelanto de Efectivo (u otro acceso a efectivo), o una Transacción de ATM completada a través de una Tarjeta.

Transacción de EMV significa la transacción de una tarjeta de circuito integrado (algunas veces denominadas como una "tarjeta IC", "tarjeta con chip", "tarjeta inteligente", "tarjeta EMV" o "ICC") llevada a cabo en un terminal de punto de venta (POS) con capacidad de procesar tarjetas IC y con una aprobación de tipo EMV válida y actual. Las aprobaciones de tipo EMV están disponibles en www.emvco.com.

Transacciones de pago iniciadas por el comprador (BIP) significa una solución de pago digital que permite a los compradores programar pagos de forma rápida y eficiente a los proveedores (vinculados a tarjetas corporativas).

Ventana de evento del Incidente de Datos significa la ventana de intrusión (o un período de tiempo determinado de igual manera) establecida en el informe forense final (por ej., Informe PFI), o, si se desconoce, hasta 365 días antes de la Fecha de la última Notificación de Números de Tarjeta potencialmente Comprometidos involucrados en un informe de Datos Comprometidos.

Sección 9 Sitios web útiles

Seguridad de los datos de American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC (Consejo de los Estándares de Seguridad de la PCI): www.pcisecuritystandards.org

EMVCo: www.emvco.com