AMERICAN EXPRESS

Política de Seguridad de Datos (DSOP)

Iconos de cambios

Las actualizaciones importantes se enumeran en la Tabla de resumen de cambios y también se indican en la *DSOP* con un icono de cambios. Un icono de cambios junto al título de una sección o subsección indica que se ha actualizado, añadido o eliminado texto de las mismas. Los cambios en la *DSOP* se indican con un icono de cambios como el que aquí se muestra.

Tabla de resumen de cambios

Las actualizaciones importantes se enumeran en la tabla siguiente y también se indican en la *DSOP* con un icono de cambios.

Sección/Subsección	Descripción del cambio
¿Qué debe hacerse en el caso de que ocurra una Incidencia de Datos?	Se han añadido los pasos que deben seguirse cuando se identifica una Incidencia de Datos.

¿Qué debe hacerse en el caso de que ocurra una Incidencia de Datos?

Siga estos pasos si ha identificado una Incidencia de Datos en su empresa.

Paso 1:

Cumplimente el Formulario de aviso inicial de Incidencia de Datos del Establecimiento y envíelo por correo electrónico a EIRP@aexp.com en un plazo de 72 horas después de descubrirse la Incidencia de Datos.

Paso 2:

Realice una investigación exhaustiva; esto puede requerir la contratación de un Investigador forense de la Industria de Tarjetas de Pago (PCI - Payment Card Industry).

Paso 3:

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

Paso 4:

Trabaje con nosotros para que podamos ayudarle a resolver los problemas derivados de la Incidencia de Datos.

Consulte la Sección 3, "Obligaciones para gestionar Incidencias de Datos", para obtener más información sobre las Obligaciones para gestionar Incidencias de Datos.

¿Tiene alguna pregunta?

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

Internacional: +1 (602) 537-3021

EIRP@aexp.com

Como líder en medidas de protección del consumidor, American Express mantiene firmemente su compromiso de proteger los Datos de Titulares de Tarjetas y los Datos Confidenciales de Autenticación, así como de guardarlos de forma segura.

Cualquier pérdida o acceso indebido a los datos puede afectar negativamente a consumidores, Establecimientos, Proveedores de Servicios y Entidades Emisoras de tarjetas. Cualquier incidencia en este sentido puede dañar gravemente la reputación de una empresa e impedir el normal desarrollo de su negocio. La implantación de políticas de seguridad de datos puede aumentar tanto la confianza de los clientes como la rentabilidad y la reputación de la empresa.

En American Express sabemos que nuestros Establecimientos y Proveedores de Servicios (denominados en adelante colectivamente **usted** o **ustedes**) comparten esta preocupación. Por ello les pedimos que, como parte de sus responsabilidades, cumplan estrictamente las normas de seguridad de datos descritas en su **Contrato** (en adelante, el Contrato) a la hora de aceptar (en el caso de Establecimientos) o de procesar (en el caso de Proveedores de Servicios) la Tarjeta American Express®, así como la presente Política de Seguridad de Datos, que está sujeta a modificaciones periódicas. Estos requisitos son aplicables a todos los equipos, sistemas y redes (y componentes de los mismos) en los que se almacenan, procesan o transmiten Claves de Cifrado, Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o una combinación de los mismos).

Los términos en mayúsculas utilizados, pero no definidos, en este documento tienen el significado explicado en el glosario incluido al final de esta política.

Sección 1 Programa de Análisis Dirigido (TAP - Targeted Analysis Program)

Los Datos de Titulares de Tarjetas pueden verse comprometidos por deficiencias de seguridad en el Entorno de Datos de Titulares de Tarjetas (CDE - Cardholder Data Environment).

Algunos ejemplos de situaciones en las que los Datos de Titulares de Tarjetas podrían verse comprometidos son, entre otros:

- **Mismo Punto de Compra (CPP - Common Point of Purchase):** Los Titulares American Express denuncian operaciones fraudulentas en las cuentas de sus Tarjetas y se identifica y determina que se han originado al realizar compras en sus Establecimientos.
- **Hallazgo de los Datos de Tarjetas de Crédito:** Se encuentran Datos de Tarjetas American Express y de Titulares de Tarjetas en Internet vinculados a operaciones realizadas en sus Establecimientos.
- **Sospecha de malware:** American Express sospecha que usted está utilizando software infectado o que es vulnerable a código malicioso.

TAP está diseñado para identificar las situaciones en las que los Datos de Titulares de Tarjetas podrían haberse visto comprometidos.

Usted debe asegurarse de que tanto usted como sus Terceros Involucrados cumplan los siguientes requisitos tras la notificación, por parte de American Express, de que los Datos de Titulares de Tarjetas podrían haberse visto comprometidos.

- Debe auditar su CDE para encontrar deficiencias de seguridad y subsanarlas.
  - Debe asegurarse de que sus proveedores externos lleven a cabo una investigación exhaustiva de su CDE si se ha subcontratado.
- Debe proporcionar un resumen de las medidas adoptadas o previstas de su auditoría, evaluación y/o esfuerzos para subsanar las deficiencias tras la notificación por parte de American Express.
- Debe proporcionar documentos de validación de PCI DSS actualizados de acuerdo con la Sección 5, "Importante Validación Periódica de sus Sistemas".
- Según corresponda, debe contratar a un Investigador Forense de PCI (PFI - PCI Forensic Investigator) cualificado para que examine su CDE si usted o sus Terceros Involucrados:
  - no son capaces de subsanar en un plazo razonable la deficiencia que ha comprometido los Datos de los Titulares de Tarjetas, según lo determine American Express, o
  - confirman que se ha producido un Incidente de Datos y cumplen con los requisitos establecidos en la Sección 3, "Obligaciones para gestionar Incidencias de Datos".

Penalizaciones por incumplimiento del programa 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
Penalización por incumplimiento cuando no se satisfagan en un plazo de 45 días a partir de la fecha de notificación las obligaciones del programa TAP.	25.000 USD	5.000 USD	1.000 USD
Penalización por incumplimiento cuando no se satisfagan en un plazo de 90 días a partir de la fecha de notificación las obligaciones del programa TAP.	35.000 USD	10.000 USD	2.500 USD
Penalización por incumplimiento cuando no se satisfagan en un plazo de 120 días a partir de la fecha de notificación las obligaciones del programa TAP. **AVISO:** *Las penalizaciones por incumplimiento pueden seguir aplicándose mensualmemente hasta que se satisfagan las obligaciones o se resuelva el incumplimiento del programa TAP.*	45.000 USD	15.000 USD	5.000 USD

Si no se satisfacen las obligaciones del programa TAP, American Express tiene derecho a imponer las penalizaciones por incumplimiento de forma acumulativa, retener pagos y/o rescindir el Contrato.

Sección 2 Normas para la protección de Claves de Cifrado, Datos de Titulares de Tarjetas y Datos Confidenciales de Autenticación

Usted debe asegurarse de que tanto usted como sus Terceros Involucrados:

- almacenen Datos de Titulares de Tarjetas exclusivamente con el fin de facilitar operaciones con Tarjetas American Express cumpliendo estrictamente los términos del Contrato,
- cumplan los requisitos de las versiones vigentes del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS - Payment Card Industry Data Security Standard) y de los Requisitos del Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC - Payment Card Industry Security Standards Council) relativos al procesamiento, almacenamiento y transmisión de Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación desde la misma fecha de entrada en vigor de dichas versiones,
- a la hora de desplegar Dispositivos para Introducción de PIN o Aplicaciones de Pago (o ambos), tanto nuevos como de sustitución, en ubicaciones atendidas, utilicen solo los Homologados por PCI.

Usted debe proteger, siguiendo estas normas de seguridad de datos, todos los registros de Cargos y Abonos de American Express conservados en el cumplimiento del Contrato; utilizará dichos registros solo para los fines estipulados en el Contrato, y los salvaguardará en consecuencia. Usted será responsable ante American Express, tanto económicamente como en todos los demás aspectos, de garantizar el cumplimiento de estas normas de protección de datos por parte de sus Terceros Involucrados (salvo para demostrar dicho cumplimiento de esta política por sus Terceros Involucrados, según se indica en la Sección 5, "Importante Validación Periódica de sus Sistemas", y salvo que en dicha sección se indique otra cosa).

Sección 3 Obligaciones para gestionar Incidencias de Datos

Usted deberá notificar a American Express cualquier Incidencia de Datos inmediatamente, y en ningún caso después de transcurridas más de setenta y dos (72) horas desde su detección.

Para avisar a American Express, llame al departamento del Programa de Respuesta ante Incidentes Empresariales de American Express (*EIRP* - American Express Enterprise Incident Response Programme) en el número +1 (602) 537-3021 (sustituya el signo "+" por el prefijo de marcación internacional directa "IDD". Son aplicables las tarifas de llamadas internacionales), o envíe un correo electrónico a EIRP@aexp.com. Usted deberá designar una persona como contacto para todo lo relacionado con la Incidencia de Datos. Asimismo:

- Usted deberá realizar una investigación exhaustiva de cada Incidencia de Datos.
- Cuando la Incidencia de Datos afecte a 10.000 o más Números de Tarjetas únicos, esta investigación deberá encomendarse a un investigador forense de PCI (PFI), quien deberá llevarla a cabo en los cinco (5) días posteriores a la detección de dicha Incidencia de Datos.
- El informe no editado de la investigación deberá facilitarse a American Express en un plazo máximo de diez (10) días laborables desde la fecha de su finalización.
- Usted deberá facilitar de inmediato a American Express todos los Números de Tarjetas Comprometidos. American Express se reserva el derecho de realizar su propio análisis interno para identificar los Números de Tarjetas afectados por la Incidencia de Datos.

Los informes de investigaciones forenses deben cumplimentarse utilizando la versión más reciente de la plantilla para informes finales de incidencias forenses de PCI. Los informes forenses de estas investigaciones deben contener análisis forenses, informes de cumplimiento de normas y cualquier otra información relacionada con la Incidencia de Datos; identificar la causa de la Incidencia de Datos; determinar si en el momento de producirse la Incidencia de Datos usted cumplía el estándar PCI DSS; y verificar su capacidad de prevenir futuras Incidencias de Datos mediante (i) la presentación de un plan de subsanación de todas las deficiencias relacionadas con el estándar PCI DSS y (ii) la participación en el programa de cumplimiento de American Express (descrito a continuación). A petición de American Express, usted deberá demostrar que las deficiencias han sido subsanadas, para lo cual deberá aportar la correspondiente certificación de un Asesor de Seguridad Certificado (QSA - Qualified Security Assessor).

Sin perjuicio de lo establecido en esta Sección 3, "Obligaciones para gestionar Incidencias de Datos":

- American Express podrá, a su entera discreción, requerirle que contrate a un PFI para que lleve a cabo una investigación sobre la Incidencia de Datos para aquellas Incidencias de Datos en las que se vean afectados menos de 10.000 Números de Tarjetas únicos. Dicha investigación debe cumplir con los requisitos establecidos anteriormente en esta Sección 3, "Obligaciones para gestionar Incidencias de Datos" y tendrá que completarse dentro del plazo de tiempo que American Express establezca.
- American Express podrá, a su entera discreción, contratar por su cuenta a un PFI para que lleve a cabo una investigación sobre la Incidencia de Datos y puede cargarle a usted el coste de la misma.

Usted cooperará con American Express en la rectificación de cualquier problema que pueda derivarse de la Incidencia de Datos, así como elaborará junto a American Express los comunicados a los Titulares afectados por la Incidencia de Datos, y facilitará a American Express toda la información pertinente (previa obtención de las autorizaciones necesarias) para que podamos verificar su capacidad de prevenir futuras Incidencias de Datos según los términos establecidos en el Contrato.

Sin perjuicio de cualquier otra obligación de confidencialidad establecida en el Contrato, American Express tendrá derecho a revelar información sobre cualquier Incidencia de Datos a Titulares de Tarjetas American Express, a Entidades Emisoras, a otros participantes de la Red de American Express y al público en general, según establezca la legislación aplicable, una orden judicial, administrativa o reglamentaria, un decreto, una citación, solicitud u otro proceso legal, con el fin de reducir el riesgo de fraude u otros daños o para garantizar la continuidad del funcionamiento de la Red de American Express.

Sección 4 Indemnización en casos de Incidencias de Datos

En esta Sección 4, "Indemnización en casos de Incidencias de Datos", se definen sus obligaciones de indemnización a American Express en el marco del Contrato en caso de producirse alguna Incidencia de Datos, sin perjuicio de los demás derechos y recursos de American Express. Aparte de la indemnización (si la hubiera), usted podría tener que pagar una penalización por incumplimiento con resultado de Incidencia de Datos tal y como se establece a continuación en esta Sección 4, "Indemnización en casos de Incidencias de Datos".

En casos de Incidencias de Datos que afecten:

- a 10.000 o más Números de Tarjeta de American Express en lo relativo a:
  - Datos Confidenciales de Autenticación, o
  - Fecha de caducidad

  usted deberá indemnizar a American Express a razón de 5 USD por cada número de cuenta.

Sin embargo, American Express no le exigirá ninguna indemnización por Incidencias de Datos que afecten:

- a menos de 10.000 Números de Tarjeta de American Express, o
- a más de 10.000 Números de Tarjeta de American Express si se cumple lo siguiente:
  - usted notificó a American Express la Incidencia de Datos cumpliendo la Sección 4, "Indemnización en casos de Incidencias de Datos", de esta política,
  - en el momento de producirse la Incidencia de Datos, usted cumplía el estándar PCI DSS (según determine la investigación del PFI sobre la Incidencia de Datos), y
  - la Incidencia de Datos no fue causada por conducta ilícita suya o de alguno de sus Terceros Involucrados.

Sin perjuicio de lo dispuesto en los párrafos anteriores de esta Sección 4, "Indemnización en casos de Incidencias de Datos", en casos de Incidencia de Datos, independientemente del número de Números de Tarjeta de American Express, usted pagará a American Express una penalización por incumplimiento con resultado de Incidencia de Datos que no superará los 100.000 USD por cada Incidencia de Datos (según el criterio establecido por American Express) en el caso de que usted no cumpla con las obligaciones establecidas en la Sección 3, "Obligaciones para gestionar Incidencias de Datos". Para evitar cualquier posible duda, la penalización total por incumplimiento con resultado de Incidencia de Datos establecida para cada caso de Incidencia de Datos individual no superará los 100.000 USD.

American Express excluirá de sus cálculos todos los Números de Cuenta de Tarjetas de American Express que se hayan visto implicados en una reclamación de indemnización anterior por Incidencia de Datos dentro de los doce (12) meses anteriores a la Fecha de Notificación. Todos los cálculos realizados por American Express con este método son definitivos.

American Express puede cobrarle el importe completo de sus obligaciones de indemnización por Incidencias de Datos o deducir el importe de los pagos de American Express a usted (o cargar el importe en su Cuenta Bancaria según corresponda) según lo establecido en el Contrato.

Sus obligaciones de indemnización en los casos de Incidencias de Datos descritos en el presente documento no tendrán la consideración de daños fortuitos, indirectos, especulativos, consecuentes, especiales, punitivos ni ejemplares según el Contrato, siempre que dichas obligaciones no incluyan los daños relacionados con la pérdida de facturación o de beneficios, la pérdida de clientes o la pérdida de oportunidades de negocio.

American Express puede, a su entera discreción, limitar su obligación de indemnización a Establecimientos exclusivamente por aquellas Incidencias de Datos que cumplan todos y cada uno de los criterios siguientes:

- Antes de que se produjera la Incidencia de Datos, se emplearon las Tecnologías de Reducción de Riesgos pertinentes, que siguieron utilizándose durante la Duración completa de la Incidencia de Datos.
- Se llevó a cabo una investigación exhaustiva en los términos establecidos en el programa para PFI (salvo que se hubiesen acordado otros términos por escrito).
- El informe forense indica claramente que las Tecnologías de Reducción de Riesgos se empleaban para procesar, almacenar y/o transmitir los datos en el momento en que se produjo la Incidencia de Datos.

- Usted no conserva (ni conservaba durante la Duración de la Incidencia de Datos) Datos Confidenciales de Autenticación ni otros Datos de Titulares de Tarjetas que no se hayan convertido en ilegibles.

Siempre que sea aplicable alguna reducción de la indemnización (sin incluir las penalizaciones por incumplimiento que puedan ser aplicables), dicha reducción se determinará del siguiente modo:

Reducción de la obligación de indemnización	Criterios requeridos
Reducción estándar: 50 %	>75 % de todas las operaciones procesadas en Dispositivos Compatibles con Chip[1], o
	Uso de Tecnologías de Reducción de Riesgos en >75 % de las ubicaciones del Establecimiento[2]
Reducción ampliada: del 75 % al 100 %	>75 % de todas las operaciones procesadas en Dispositivos Compatibles con Chip[1] y uso de otras Tecnologías de Reducción de Riesgos en >75 % de las ubicaciones del Establecimiento[2]

[1] Según determinen los análisis internos de American Express

[2] Según determine la investigación del PFI

- La reducción ampliada (del 75 % al 100 %) se determinará en función del menor de los porcentajes de operaciones efectuadas en Dispositivos Compatibles con Chip y las ubicaciones del Establecimiento equipadas con otras Tecnologías de Reducción de Riesgos. A continuación, encontrará algunos ejemplos para calcular la reducción de la indemnización.
- Para que una tecnología se considere Tecnología de Reducción de Riesgos, usted debe demostrar que la utiliza de forma eficaz y conforme a su diseño y finalidad. Por ejemplo, instalar Dispositivos Compatibles con Chip y procesar las Tarjetas Chip a través de la Banda Magnética o la Clave NO se considera un uso eficaz de esta tecnología.
- El porcentaje de Establecimientos que emplean alguna Tecnología de Reducción de Riesgos se determina en la investigación del PFI.
- La reducción en la obligación de indemnización no es aplicable a las penalizaciones por incumplimientos de normas que puedan derivarse de la Incidencia de Datos.

Reducción ampliada de la obligación de indemnización

Ej.	Tecnologías de reducción de riesgos utilizadas	Apto	Reducción
1	80 % de las Operaciones en Dispositivos Compatibles con Chip 0 % de las ubicaciones utiliza otras Tecnologías de Reducción de Riesgos	No	50 %: Reducción estándar (un porcentaje inferior al 75 % de uso de Tecnologías de Reducción de Riesgos no se considera apto para una reducción ampliada)[1]
2	80 % de las Operaciones en Dispositivos Compatibles con Chip 77 % de las ubicaciones utiliza otras Tecnologías de Reducción de Riesgos	Sí	77 %: Reducción ampliada (basada en un uso de Tecnologías de Reducción de Riesgos del 77 %)
3	93 % de las Operaciones en Dispositivos Compatibles con Chip 100 % de las ubicaciones utiliza otras Tecnologías de Reducción de Riesgos	Sí	93 %: Reducción ampliada (basada en que un 93 % las operaciones se realizan en Dispositivos Compatibles con Chip)

Ej.	Tecnologías de reducción de riesgos utilizadas	Apto	Reducción
4	40 % de las Operaciones en Dispositivos Compatibles con Chip 90 % de las ubicaciones utiliza otras Tecnologías de Reducción de Riesgos	No	50 %: Reducción estándar (si menos del 75 % de las operaciones se realiza en Dispositivos Compatibles con Chip, no se considera apto para una reducción ampliada)

[1] Una Incidencia de Datos que afecte a 10.000 Cuentas asociadas a Tarjetas American Express, a razón de 5 USD por número de cuenta (10.000 × 5 USD = 50.000 USD) puede ser apta para una reducción del 50 %, pasando las obligaciones de indemnización de 50.000 USD a 25.000 USD, sin incluir las penalizaciones por incumplimiento.

Sección 5 Importante Validación Periódica de sus Sistemas

Usted deberá realizar las acciones siguientes para verificar su cumplimiento del estándar PCI DSS anual y trimestralmente, tal y como se describe a continuación. Tanto en sus propias instalaciones como en las de sus Franquiciados, deberá verificarse el estado de los equipos, sistemas y/o redes (y de sus componentes) en los que se almacenen, procesen o transmitan Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación.

Para realizar la validación deberá realizar estas cuatro acciones:

Acción 1: Participar en el Programa de Cumplimiento de American Express descrito en este documento.

Acción 2: Conocer su Nivel y los Requisitos de Validación correspondientes.

Acción 3: Cumplimentar la Documentación de Validación que deberá enviar a American Express.

Acción 4: Enviar la Documentación de Validación a American Express dentro de los plazos indicados.

Acción 1: Participar en el Programa de Cumplimiento de American Express descrito en este documento

Los Establecimientos de Nivel 1, Establecimientos de Nivel 2 y todos los Proveedores de Servicios, como se indica más adelante, deberán participar en el Programa de Cumplimiento PCI de American Express en los términos establecidos en este documento, debiendo indicar el nombre completo, la dirección de correo electrónico, el número de teléfono y la dirección de correo postal de la persona que actuará como su contacto general para cuestiones relacionadas con la protección de datos. Usted debe facilitar estos datos a SecureTrust, un departamento de Trustwave (https://portal.securetrust.com), que administra el programa en nombre de American Express, utilizando uno de los métodos enumerados en la Acción 4: "Enviar la Documentación de Validación a American Express" a continuación. Usted deberá avisar a SecureTrust cada vez que estos datos cambien y proporcionar los datos actualizados que correspondan. El hecho de que no nos proporcione dichos datos de contacto no afecta en modo alguno a nuestro derecho a establecer penalizaciones por no validación según lo establecido en la Tabla de penalizaciones por no validación.

American Express puede determinar, a su entera discreción y mediante notificación escrita, que determinados Establecimientos de Nivel 3 y Nivel 4 se inscriban en el Programa de Cumplimiento de American Express de acuerdo con esta política. El Establecimientos deberá inscribirse en un plazo máximo de 90 días contados desde la fecha de recepción de dicha notificación.

Acción 2: Conocer su Nivel y los Requisitos de Validación correspondientes

Existen cuatro niveles para Establecimientos y dos niveles para Proveedores de Servicios, definidos por el volumen de las operaciones realizadas con Tarjetas American Express. En el caso de los Establecimientos, se trata del volumen generado por sus Establecimientos, acumulable hasta alcanzar el nivel máximo de cuenta de Establecimiento de American Express.* Usted será asignado a uno de los Niveles especificados en las tablas de Establecimientos y Proveedores de Servicios que se incluyen más adelante. A la hora de determinar el nivel y los requisitos de

validación de un Establecimiento, no se incluyen en el volumen de operaciones con Tarjetas American Express las operaciones correspondientes a pagos Iniciados por Compradores (BIP - Buyer Initiated Payments).

* En el caso de los Franquiciadores, esto incluye el volumen correspondiente a sus establecimientos Franquiciados. Los Franquiciadores que impongan a sus Franquiciados el uso de un determinado Proveedor de Servicios o Sistema de Puntos de Venta (POS - Point of Sale) también deberán facilitar la documentación de validación relativa a los Franquiciados que correspondan.

Requisitos para Establecimientos

Los Establecimientos (no los Proveedores de Servicios) pueden ser asignados a cuatro categorías diferentes en cuanto a nivel y requisitos de validación. Una vez determinado su nivel de Establecimiento en la lista siguiente, consulte la Tabla de Establecimientos para averiguar los requisitos de documentación de validación.

- **Establecimiento de Nivel 1:** 2,5 millones o más de Operaciones anuales con Tarjetas American Express, o cualquier Establecimiento al que American Express, según su criterio, considere de Nivel 1.
- **Establecimiento de Nivel 2:** Entre 50.000 y 2,5 millones de Operaciones anuales con Tarjetas American Express.
- **Establecimiento de Nivel 3:** Entre 10.000 y 50.000 Operaciones anuales con Tarjetas American Express.
- **Establecimiento de Nivel 4:** Menos de 10.000 Operaciones anuales con Tarjetas American Express.

Tabla de Establecimientos

	Documentación de Validación		
Nivel de Establecimiento/ Operaciones anuales con American Express	Informe de Evaluación In Situ de Cumplimiento (ROC)	Cuestionario de Autoevaluación (SAQ) y análisis trimestral de la red	Certificación STEP para Establecimientos susceptibles de acogerse a este programa
Nivel 1/ 2,5 millones o más	Obligatorio	No procede	Opcional (sustituye al ROC)
Nivel 2/ 50.000 a 2,5 millones	Opcional	SAQ obligatorio (salvo que se envíe una evaluación in situ). Análisis obligatorio con ciertos tipos de SAQ	Opcional (sustituye al SAQ y al análisis de la red o ROC)
Nivel 3/ 10.000 a 50.000	Opcional	SAQ opcional (obligatorio si American Express lo solicita). Análisis obligatorio con ciertos tipos de SAQ	Opcional (sustituye al SAQ y al análisis de la red o ROC)
Nivel 4/ 10.000 o menos	Opcional	SAQ opcional (obligatorio si American Express lo solicita). Análisis obligatorio con ciertos tipos de SAQ	Opcional (sustituye al SAQ y al análisis de la red o ROC)

* Para evitar cualquier posible duda, los Establecimientos de Nivel 3 y de Nivel 4 no necesitan presentar Documentación de Validación a menos que así lo requiera American Express, aunque sí deben cumplir todas las disposiciones de esta Política de Seguridad de Datos y asumir las responsabilidades que de ella se derivan.

American Express podrá comprobar la exactitud y la adecuación de la documentación de validación de PCI proporcionada, según sea necesario, pudiendo incluso contratar los servicios de un QSA o PFI de nuestra elección, cuyos gastos correrán a cargo de American Express.

Programa de Mejora de las Tecnologías de Seguridad (STEP)

Los Establecimientos que cumplan los términos de PCI DSS también podrán, a la entera discreción de American Express, incorporarse al Programa de Mejora de las Tecnologías de Seguridad (STEP - Security Technology Enhancement Programme) de American Express siempre que implementen determinadas tecnologías de seguridad adicionales en todos sus entornos de procesamiento de Tarjetas. Solo es posible acogerse a los beneficios de STEP si el Establecimiento no ha experimentado ninguna Incidencia de Datos en los 12 meses anteriores y si al menos el 75 % de todas las operaciones con Tarjetas se realizan utilizando:

- **Tecnología EMV:** en Dispositivos Compatibles con Chip que disponen de una homologación/certificación válida y vigente de EMVCo (www.emvco.com) y que permiten procesar Operaciones con Tarjetas Chip conformes a la especificación AEIPS. (Los establecimientos de EE. UU. deben incluir tecnología Contactless)
- **Cifrado Punto a Punto (P2PE - Point-to-Point Encryption):** se comunica al procesador del Establecimiento mediante un sistema de Cifrado Punto a Punto aprobado por PCI SSC o por un QSA.

Los Establecimientos que pueden beneficiarse del STEP deben cumplir menos requisitos en cuanto a la Documentación de Validación de PCI, según se indica a continuación en la Acción 3: "Cumplimentar la Documentación de Validación que deberá enviar a American Express".

Requisitos para Proveedores de Servicios

Los Proveedores de Servicios (no los Establecimientos) pueden ser asignados a dos categorías diferentes en cuanto a nivel y requisitos de validación. Una vez determinado su nivel de Proveedor de Servicios en la lista siguiente, consulte la Tabla de Proveedores de Servicios para averiguar los requisitos de documentación de validación.

Proveedor de Servicios de Nivel 1: 2,5 millones o más de Operaciones anuales con Tarjetas American Express o cualquier Proveedor de Servicios al que American Express considere de Nivel 1.

Proveedor de Servicios de Nivel 2: Menos de 2,5 millones de Operaciones anuales con Tarjetas American Express, o cualquier Proveedor de Servicios al que American Express no considere de Nivel 1.

Los Proveedores de Servicios no pueden acogerse al Programa STEP.

Tabla de Proveedores de Servicios

Nivel	Documentación de Validación	Requisito
1	Informe de Cumplimiento sobre la Evaluación Anual de Seguridad in Situ.	Obligatorio
2	SAQ D anual (Proveedor de Servicios) y Análisis Trimestral de la Red, o bien Informe de Cumplimiento sobre la Evaluación Anual de Seguridad in Situ, si se prefiere	Obligatorio

Es recomendable que los Proveedores de Servicios también superen la Validación Adicional de Entidades Designadas de PCI.

Acción 3: Cumplimentar la Documentación de Validación que deberá enviar a American Express

Los diferentes niveles de Establecimientos y Proveedores de Servicios enumerados en las respectivas tablas de Establecimientos y de Proveedores de Servicios deberán aportar los siguientes documentos:

Evaluación Anual de Seguridad In Situ: Este informe sobre la evaluación anual de seguridad es un análisis in situ detallado de los equipos, sistemas y redes (y de sus componentes) utilizados para almacenar, procesar o transmitir Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o ambos). Debe ser realizado por:

- un QSA o por
- usted, y seguidamente ser certificado por su director ejecutivo, director financiero, director de seguridad informática o responsable principal y ser enviado anualmente a American Express en el correspondiente Certificado de Cumplimiento (AOC - Attestation of Compliance).

El AOC deberá respaldar el cumplimiento de todos los requisitos del estándar PCI DSS y, si así se le solicita, ir acompañado de copias del informe de cumplimiento completo (Establecimientos de Nivel 1 y Proveedores de Servicios de Nivel 1).

Cuestionario de Autoevaluación Anual: Este informe de autoevaluación anual es un proceso basado en el cuestionario de PCI DSS SAQ, que permite realizar una autoevaluación de los equipos, sistemas y redes (y de sus componentes) utilizados para almacenar, procesar o transmitir Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o ambos). Debe ser realizado por usted y certificado por su director ejecutivo, director financiero, director de seguridad informática o responsable principal. La sección AOC del SAQ debe presentarse anualmente a American Express. La sección AOC del SAQ debe certificar que usted cumple todos los requisitos del estándar PCI DSS y, si así se le solicita, ir acompañada de copias completas del SAQ (Establecimientos de Nivel 2, Nivel 3 y Nivel 4, y Proveedores de Servicios de Nivel 2).

Análisis Trimestral de la Red: Este análisis trimestral de la red es un proceso de exploración remota de posibles puntos débiles y vulnerabilidades en sus redes informáticas y servidores web conectados a internet. Debe ser ejecutado por un Proveedor de Análisis Autorizado (**ASV** - Approved Scanning Vendor). Usted deberá cumplimentar y enviar trimestralmente a American Express el informe del Certificado de Cumplimiento del Análisis del ASV (**AOSC** - Attestation of Scan Compliance) o el resumen ejecutivo de resultados del análisis (junto con copias del análisis completo, si se le solicitan). Mediante el AOSC o resumen ejecutivo se certifica que los resultados se obtuvieron ajustándose a los procedimientos de exploración de PCI DSS, que no se han identificado problemas de alto riesgo y que el análisis se ha superado favorablemente o se ajusta a la norma (todos los Establecimientos salvo los que también envíen un Informe de Evaluación de la Seguridad In Situ, los Establecimientos susceptibles de acogerse al programa STEP y todos los Proveedores de Servicios). Para evitar cualquier posible duda, los análisis trimestrales de la red son obligatorios si así lo exige el SAQ pertinente.

Documentación de Validación de la Certificación Anual del Programa STEP: La Certificación Anual de Cualificación STEP de American Express ("Certificación de STEP") solo está disponible para los Establecimientos que cumplan lo estipulado en la Acción 2: "Conocer su Nivel y los Requisitos de Validación correspondientes". La Certificación de STEP es un proceso que, sobre la base de los requisitos de PCI DSS, permite realizar una autoevaluación de sus equipos, sistemas y redes (y de sus componentes) en los que se almacenan, procesan o transmiten Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o ambos). Debe ser realizado por usted y certificado por su director ejecutivo, director financiero, director de seguridad informática o responsable principal. El proceso debe completarse enviando el formulario de Certificación de STEP a American Express con una periodicidad anual. (Solo Establecimientos susceptibles de acogerse al programa STEP). El formulario de Certificación Anual del Programa STEP se puede descargar del portal seguro de SecureTrust.

Incumplimiento del estándar PCI DSS: Si usted no cumple los requisitos del estándar PCI DSS, deberá cumplimentar uno de los siguientes documentos:

- Un Certificado de Cumplimiento (AOC) que incluya la Parte 4: "Plan de acción para el estado de incumplimiento".
- Un resumen generado por la herramienta de enfoque prioritario PCI y un Certificado de Cumplimiento (PASAOC - Prioritized Approach Tool Summary and Attestation of Compliance).
- Una plantilla del plan del proyecto (descargable del portal seguro de SecureTrust).

En cada uno de los documentos anteriores se deberá indicar una fecha de subsanación, que no podrá superar 12 meses contados desde la fecha de finalización del documento para ajustarse al cumplimiento normativo. Usted deberá enviar a American Express el documento correspondiente utilizando uno de los métodos enumerados más adelante en la Acción 4: "Enviar la Documentación de Validación a American Express". Usted deberá informar periódicamente a American Express sobre sus avances obtenidos en la subsanación de su estado de incumplimiento (Establecimientos de Nivel 1, Nivel 2, Nivel 3 y Nivel 4; y todos los Proveedores de Servicios). Para evitar cualquier posible duda, los Establecimientos que no cumplan los requisitos de PCI DSS no se podrán acoger al Programa STEP. Aunque American Express no le impondrá penalizaciones por no validación (descritas más abajo) por los incumplimientos que se hayan producido con anterioridad a la fecha de subsanación, usted seguirá siendo responsable ante American Express de todas las obligaciones de indemnización derivadas de cualquier posible Incidencia de Datos y deberá cumplir todas las demás disposiciones de esta política.

Acción 4: Enviar la Documentación de Validación a American Express

Todos los Establecimientos y Proveedores de Servicios a los que se requiera participar en el Programa de Cumplimiento PCI de American Express deben enviar la Documentación de Validación marcada como "obligatoria" en las tablas de la Acción 2: "Conocer su Nivel y los Requisitos de Validación correspondientes". Usted deberá presentar su Documentación de Validación a SecureTrust mediante uno de estos métodos:

- **Portal seguro:** La Documentación de Validación se puede transmitir a través del portal seguro de SecureTrust en la dirección https://portal.securetrust.com.

  Puede solicitar a SecureTrust las instrucciones de uso de este portal llamando al teléfono correspondiente para su País o enviando un correo electrónico a americanexpresscompliance@securetrust.com.
- **Fax seguro:** La Documentación de Validación se puede enviar por fax a: +1 (312) 276-4019. (sustituya el signo "+" por el prefijo de marcación internacional directa "IDD". Son aplicables las tarifas de llamadas internacionales).

  Indique su nombre, nombre legal, su nombre comercial, el nombre de su contacto responsable de la seguridad de datos, su dirección, su número de teléfono y, solo en el caso de Establecimientos, su Número de Establecimiento de American Express de 10 dígitos.

Si tiene preguntas de carácter general sobre el programa o sobre el proceso descritos anteriormente, póngase en contacto con SecureTrust llamando al + 800 9000 1140 o al +1 (312) 267-3208 o enviando un correo electrónico a americanexpresscompliance@securetrust.com.

Usted correrá con todos los gastos de cumplimiento y validación. En el momento de presentar la Documentación de Validación, usted declara y garantiza a American Express que está autorizado a revelar la información contenida en dicha Documentación de Validación y que se la proporciona a American Express sin violar los derechos de ninguna otra parte.

Mercados	Número de teléfono de SecureTrust
Alemania	+ 800 9000 1140
Argentina	+ 800 9000 1140
Australia	+ 800 9000 1140
Austria	+ 800 9000 1140
Bulgaria	+ 312 267 3208
Canadá	1 866 659 9016
Chipre	+ 800 9000 1140
Croacia	+ 312 267 3208
Dinamarca	+ 800 9000 1140
Eslovaquia	+ 312 267 3208
Eslovenia	+ 312 267 3208
España	+ 800 9000 1140
Estados Unidos	1 866 659 9016
Estonia	+ 312 267 3208
Francia	+ 800 9000 1140

Mercados	Número de teléfono de SecureTrust
Grecia	+ 312 267 3208
Hong Kong	+ 800 9000 1140
Hungría	+ 800 9000 1140
IDC	+ 888 900 0114
India	+ 000 800 100 1177
Irlanda	+ 800 9000 1140
Islandia	+ 800 9000 1140
Italia	+ 800 9000 1140
Japón	+ 312 267 3208
Letonia	+ 312 267 3208
Lituania	+ 312 267 3208
Malta	+ 312 267 3208
México	+ 888 900 0114
Noruega	+ 800 9000 1140
Nueva Zelanda	+ 800 9000 1140
Países Bajos	+ 312 267 3208
Polonia	+ 800 9000 1140
Portugal	+ 312 267 3208
Reino Unido	+ 800 9000 1140
República Checa	+800 144 316
Rumanía	+ 312 267 3208
Rusia	+ 312 267 3208
Singapur	+ 800 9000 1140
Suecia	+ 800 9000 1140
Tailandia	+ 800 9000 1140
Taiwán	+ 312 267 3208

Sustituya el signo "+" por el prefijo de marcación internacional directa "IDD". Son aplicables las tarifas de llamadas internacionales

Penalizaciones por no validación y Terminación del Contrato

American Express tendrá derecho a imponerle penalizaciones por no validación y a terminar el Contrato si usted incumple estos requisitos o no proporciona la Documentación de Validación obligatoria a American Express dentro del plazo establecido. American Express le comunicará individualmente el plazo establecido para cada periodo de comunicación anual y trimestral.

Envíe la documentación a American Express en el plazo establecido correspondiente. American Express le comunicará individualmente el plazo establecido para cada periodo de comunicación anual y trimestral.

Tabla de penalizaciones por no validación

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 cobrará una penalización por no validación si la Documentación de Validación no se recibe dentro del primer plazo establecido.	25.000 USD	5.000 USD	50 USD
Se cobrará una penalización adicional por no validación si la Documentación de Validación no se recibe dentro de los 60 días siguientes al primer plazo establecido.	35.000 USD	10.000 USD	100 USD
Se cobrará una penalización adicional por no validación si la Documentación de Validación no se recibe dentro de los 90 días siguientes al primer plazo establecido y cada 30 días en lo sucesivo.	45.000 USD	15.000 USD	250 USD

* Las penalizaciones por no validación se calcularán en el equivalente en la divisa local.

** No aplicable en Argentina.

Si American Express no recibe su Documentación de Validación obligatoria dentro de los 90 días siguientes al primer plazo establecido, American Express podrá terminar el Contrato en los términos establecidos en el mismo, así como imponerle el pago de las penalizaciones por no validación acumulativas indicadas.

Sección 6 Confidencialidad

American Express adoptará (e impondrá a sus agentes y subcontratistas, como SecureTrust, que adopten) medidas razonables para mantener la confidencialidad de sus informes de cumplimiento, incluida la Documentación de Validación, así como para impedir la divulgación de la Documentación de Validación a terceros (salvo a afiliados, agentes, representantes, Proveedores de Servicios y subcontratistas de American Express) durante un plazo de tres años contados desde la fecha de su recepción. Este compromiso de confidencialidad no será aplicable a la Documentación de Validación que:

a. American Express ya conociera antes de su divulgación,

b. deje de ser confidencial y pase a ser de dominio público sin que American Express haya incumplido los términos de este párrafo,

c. American Express haya recibido legítimamente de un tercero sin obligación de confidencialidad,

d. American Express haya generado por su cuenta, o

e. cuya divulgación se deba al cumplimiento de una orden judicial, administrativa o gubernamental, de cualquier ley, disposición o reglamentación, de una citación, petición de documentación u otro proceso administrativo o legal, o de cualquier investigación o petición de información formal o informal por parte de cualquier organismo o autoridad oficial (reguladores, inspectores, evaluadores o agencias de orden público).

Sección 7 Exención de responsabilidad

POR LA PRESENTE, AMERICAN EXPRESS DECLINA TODA RESPONSABILIDAD Y/O GARANTÍA ASUMIDA O RELACIONADA CON ESTA POLÍTICA DE SEGURIDAD DE DATOS, CON EL ESTÁNDAR PCI DSS, CON LAS ESPECIFICACIONES EMV Y CON LA DESIGNACIÓN Y EL RENDIMIENTO DE CUALQUIER QSA, ASV O PFI, TANTO EXPRESA COMO IMPLÍCITA, LEGAL O DE CUALQUIER OTRO TIPO, INCLUSO TODA GARANTÍA DE IDONEIDAD PARA UN FIN EN PARTICULAR. LAS ENTIDADES EMISORAS DE TARJETAS AMERICAN EXPRESS NO SON TERCEROS BENEFICIARIOS DE ESTA POLÍTICA.

Sitios web útiles

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

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Glosario

Las siguientes definiciones serán aplicables exclusivamente a efectos de esta Política de Seguridad de Datos (DSOP) en caso de que se produzca algún conflicto con los términos contenidos en las *Reglamentaciones para Establecimientos*.

Abono es el importe equivalente al Cargo reembolsado a Titulares American Express por compras o pagos realizados con la Tarjeta.

Aplicación de Pago tendrá en cada momento el significado indicado en el Glosario del Estándar de Seguridad de Datos de Aplicación de Pago de la Industria de Tarjetas de Pago ("Payment Card Industry Payment Application Data Security Standard"), disponible en www.pcisecuritystandards.org.

Asesor de seguridad Certificado (QSA - Qualified Security Assessor) es una entidad homologada por Payment Card Industry Security Standards Council, LLC para verificar el grado de cumplimiento del estándar PCI DSS.

Cargo es un pago o una compra que se ha realizado con una Tarjeta.

Certificado de Cumplimiento (AOC - Attestation of Compliance) es una declaración que describe el grado de cumplimiento del estándar PCI DSS, en el formato proporcionado por Payment Card Industry Security Standards Council, LLC.

Certificado de Cumplimiento del Análisis (AOSC - Attestation of Scan Compliance) es una declaración que describe el grado de cumplimiento del estándar PCI DSS, basándose en un análisis de red, en el formato proporcionado por Payment Card Industry Security Standards Council, LLC.

Chip es un microchip integrado incrustado en una Tarjeta. Contiene los datos del Titular de la Tarjeta y la información de la cuenta asociada.

Cifrado Punto a Punto (P2PE - Point-to-Point Encryption) se refiere a una solución que protege criptográficamente los datos de la cuenta desde el momento en que un establecimiento acepta la tarjeta de pago hasta el punto de descifrado seguro.

Clave de Cifrado (clave de cifrado de American Express) se refiere a todas las claves utilizadas para el procesamiento, la generación, la carga y/o la protección de los datos de cuenta. Abarca los siguientes tipos de claves, aunque sin limitarse a ellos:

- Claves de cifrado: ZMKs ("Zone Master Keys") y ZPKs ("Zone Pin Keys")
- Claves maestras utilizadas en dispositivos criptográficos seguros: LMKs ("Local Master Keys")
- CSCKs ("Card Security Code Keys")
- Claves de PIN: BDKs ("Base Derivation Keys"), PEKs ("PIN Encryption Key") y ZPKs

Cuestionario de Autoevaluación (SAQ - Self-Assessment Questionnaire) es un cuestionario de autoevaluación creado por Payment Card Industry Security Standards Council, LLC para evaluar y certificar la conformidad con el estándar PCI DSS.

Datos Confidenciales de Autenticación tiene el significado descrito en la versión vigente en cada momento del Glosario del estándar PCI DSS.

Datos de Titulares de Tarjetas es la información de los Titulares American Express y de las operaciones que realizan con dichas Tarjetas: nombres, direcciones, números de las cuentas asociadas a las tarjetas y números de identificación de las tarjetas (CIDs).

Datos de Titulares de Tarjetas tiene el significado descrito en la versión vigente en cada momento del Glosario del estándar PCI DSS.

Dispositivo Compatible con Chip es un dispositivo de punto de venta que dispone de una homologación/certificación válida y vigente de EMVCo (www.emvco.com) y que permite procesar operaciones con Tarjetas Chip conformes con la especificación AEIPS.

Dispositivo de Introducción de PIN tendrá en cada momento el significado indicado en el Glosario de Seguridad en las Operaciones con PIN de la Industria de Tarjetas de Pago (PTS - Payment Card Industry PIN Transaction Security), Puntos de Interacción (POI - Point of Interaction), Requisitos de Seguridad Modular, disponible en www.pcisecuritystandards.org.

Documentación de Validación es la certificación AOC presentada con la Evaluación Anual de Seguridad In Situ o SAQ, la AOSC y los resúmenes de los resultados obtenidos por los análisis trimestrales de la red "Quarterly Network Scans" o por la Certificación Anual del Programa de Mejora de las Tecnologías de Seguridad.

Duración de la Incidencia de Datos es el periodo de tiempo que comienza en la fecha en que se produjo el uso fraudulento, si se conoce, o 365 días antes de la Fecha de Notificación, en caso de no conocerse la fecha del uso fraudulento. La Duración de la Incidencia de Datos termina 30 días después de la Fecha de Notificación.

Entidad Emisora es la Entidad (incluyendo American Express y sus Afiliados) con licencia de American Express o de un Afiliado de American Express para emitir Tarjetas y participar en el negocio de emisión de Tarjetas.

Entorno de Datos de Titulares de Tarjetas (CDE - Cardholder Data Environment) abarca a las personas, procesos y tecnología que guardan, procesan o transmiten Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación.

Especificaciones EMV son las especificaciones elaboradas por EMVCo, LLC y disponibles en www.emvco.com.

Establecimiento se refiere a cualquier Establecimiento y a los afiliados del mismo que acepta Tarjetas American Express en virtud de un Contrato firmado con American Express o con sus afiliados.

Establecimiento de Nivel 1: 2,5 millones o más de Operaciones anuales con Tarjetas American Express, o cualquier Establecimiento al que American Express considere de Nivel 1.

Establecimiento de Nivel 2: Entre 50.000 y 2,5 millones de Operaciones anuales con Tarjetas American Express.

Establecimiento de Nivel 3: Entre 10.000 y 50.000 Operaciones anuales con Tarjetas American Express.

Establecimiento de Nivel 4: Menos de 10.000 Operaciones anuales con Tarjetas American Express.

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS - Payment Card Industry Data Security Standard) es el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago que está disponible en www.pcisecuritystandards.org.

Fecha de Notificación es la fecha en que American Express realiza la notificación final de una Incidencia de Datos a las Entidades Emisoras. Dicha fecha está supeditada a la recepción del informe forense o el análisis interno definitivos por parte de American Express, y será determinada exclusivamente por American Express.

Franquiciado es un tercero de titularidad y actividad independiente (incluido un franquiciado, licenciatario o delegado) que no sea un Afiliado que tiene licencia de un Franquiciador para operar una franquicia y que ha suscrito un contrato por escrito con el Franquiciador por el cual muestra una identificación externa visible que le identifica claramente con las Marcas del Franquiciador o que se presenta al público como un miembro del grupo de empresas del Franquiciador.

Franquiciador es el operador de una empresa que concede licencias a personas o a Entidades (Franquiciados) para distribuir bienes y/o servicios en nombre de la Marca del operador o utilizando dicha marca; proporciona asistencia a los Franquiciados en cuanto a la operativa de su negocio o influye en la forma de funcionamiento del Franquiciado; y cobra una comisión a los Franquiciados.

Homologado por PCI significa que, en el momento de la implementación, la lista de empresas y proveedores homologados por PCI Security Standards Council, LLC contiene un determinado Dispositivo de Introducción de PIN o una determinada Aplicación de Pago (o ambos). Dicha lista está disponible en www.pcisecuritystandards.org.

Incidencia de Datos se refiere a una incidencia de uso fraudulento (presunto o demostrado) de claves de cifrado de American Express, o de al menos un número de cuenta asociado a una Tarjeta American Express en el que se produzca un:

- acceso o uso no autorizado de Claves de Cifrado, Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o una combinación de ellos) almacenados, procesados o transmitidos mediante equipos, sistemas y/o redes (o sus componentes) que sean de su propiedad o sobre los que usted tenga potestad de uso, o que usted ofrezca o ponga a disposición de otras partes;
- uso no conforme con el Contrato de dichas Claves de Cifrado, Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o una combinación de ellos); y/o
- sospecha o confirmación de pérdida, robo o apropiación indebida por cualquier método o medio de cualquier soporte, material, registro o información que contenga dichas Claves de Cifrado, Datos de Titulares de Tarjetas o Datos Confidenciales de Autenticación (o una combinación de ellos).

Investigador forense de PCI (PFI - PCI Forensic Investigator) es una entidad autorizada por la Payment Card Industry Security Standards Council, LLC para realizar investigaciones forenses en casos de incumplimiento de normas o violación de los datos de tarjetas de pago.

Número de Tarjeta es el número de identificación único que la Entidad Emisora asigna a la Tarjeta al emitirla.

Número de Tarjeta Comprometido es el número de la cuenta asociada a la Tarjeta American Express involucrada en una Incidencia de Datos.

Operación es un Cargo o Abono realizado por medio de una Tarjeta.

Operación EMV se refiere a operaciones realizadas mediante tarjetas con circuito integrado (también conocidas como "tarjetas IC", "tarjetas chip", "tarjetas inteligentes", "tarjetas EMV" o simplemente "ICC") en Terminales Punto de Venta (POS) compatibles con tarjetas IC que dispongan de una homologación EMV válida y vigente. Las homologaciones de tipo EMV están disponibles en www.emvco.com.

Operaciones correspondientes a Pagos Iniciados por Compradores (BIP - Buyer Initiated Payment) son operaciones de pago habilitadas a través de ficheros de instrucciones de pago procesados mediante BIP.

PCI DSS es el acrónimo del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago ("Payment Card Industry Data Security Standard"), que está disponible en www.pcisecuritystandards.org.

Procesador es un proveedor de servicios para Establecimientos que facilita el procesamiento de autorizaciones y transmisión a la red de American Express.

Programa de Análisis Dirigido es un programa que proporciona una alerta temprana en el caso de que los Datos de Titulares de Tarjetas pudieran haberse visto comprometidos en el Entorno de Datos de Titulares de Tarjetas (CDE). Consulte la Sección 1, "Programa de Análisis Dirigido (TAP - Targeted Analysis Program)".

Programa de Mejora de las Tecnologías de Seguridad (STEP - Security Technology Enhancement Programme) es el programa de American Express pensado para animar a los Establecimientos a implementar tecnologías que mejoren la seguridad de los datos. Para poder acogerse al programa STEP, los Establecimientos no deben haber sufrido Incidencias de Datos en los 12 meses anteriores a la presentación de la Certificación Anual de STEP y han de realizar al menos el 75 % de sus operaciones mediante Cifrado Punto a Punto o personalmente con Dispositivos Compatibles con Chip y tecnología EMV.

Proveedor de Análisis Autorizado (ASV - Approved Scanning Vendor) es una Entidad autorizada por Payment Card Industry Security Standards Council, LLC para comprobar el cumplimiento de determinados requisitos del estándar PCI DSS mediante análisis de vulnerabilidad de entornos conectados a internet.

Proveedores de Servicios son procesadores autorizados, procesadores ajenos, proveedores de pasarelas, integradores de Sistemas de Puntos de Venta (POS) y cualesquiera otros proveedores que suministran Sistemas de POS u otras soluciones o servicios de procesamiento de pagos a Establecimientos.

Proveedor de Servicios de Nivel 1: 2,5 millones o más de Operaciones anuales con Tarjetas American Express o cualquier Proveedor de Servicios al que American Express considere de Nivel 1.

Proveedor de Servicios de Nivel 2: Menos de 2,5 millones de Operaciones anuales con Tarjetas American Express, o cualquier Proveedor de Servicios al que American Express no considere de Nivel 1.

Requisitos de Payment Card Industry Security Standards Council (PCI SSC) se refiere al conjunto de estándares y requisitos relativos a la seguridad y protección de los datos de tarjetas de pago, incluidos el PCI DSS y el PA DSS, disponibles en www.pcisecuritystandards.org.

Requisitos de Seguridad PCI PIN son requisitos de seguridad relativos al PIN de la industria de tarjetas de pago. Se pueden descargar en www.pcisecuritystandards.org.

Sistema de Puntos de Venta (POS - Point of Sale) es un sistema o equipo de procesamiento de información, compuesto por un terminal, un ordenador personal, una caja registradora electrónica, un lector sin contacto o un motor o proceso de pagos, utilizado por un Establecimiento para obtener autorizaciones o para registrar datos de operaciones, o para ambos fines.

Solución aprobada de Cifrado Punto a Punto (P2PE - Point-to-Point Encryption), incluida en la lista de soluciones validadas PCI SSC o validada por una Empresa P2PE Asesora de Seguridad Autorizada por PCI SSC.

Tarjeta American Express, o **Tarjeta**, se refiere a cualquier tarjeta, dispositivo de acceso a cuentas o dispositivo o servicio de pago que lleve un nombre de afiliado, logotipo, marca registrada, marca de servicio, nombre comercial u otro diseño o denominación de American Express y que haya sido emitido por una Entidad Emisora o un número de cuenta asociado a una tarjeta.

Tarjeta Chip es una Tarjeta que contiene un Chip y puede solicitar la introducción de un número PIN para verificar la identidad del Titular de la Tarjeta o la información de cuenta que consta en el Chip, o ambos datos (en nuestra documentación también solemos denominarla "tarjeta inteligente", "tarjeta EMV", "ICC" o "tarjeta con circuito integrado").

Titular de Tarjeta es una persona o entidad que (i) ha suscrito un acuerdo con una Entidad Emisora para crear una cuenta asociada a su Tarjeta o (ii) cuyo nombre figura en la Tarjeta.

Tecnologías de Reducción de Riesgos son soluciones tecnológicas que mejoran la seguridad de los Datos de Titulares de Tarjetas y los Datos Confidenciales de Autenticación de American Express, según lo determinado por American Express. Para que una tecnología se considere Tecnología de Reducción de Riesgos, usted debe demostrar que la utiliza de forma eficaz y conforme a su diseño y finalidad. Algunos ejemplos incluyen: la tecnología EMV, el Cifrado Punto a Punto y la tokenización.

Terceros Involucrados se refiere a cualquier empleado, agente, representante, subcontratista, Procesador, Proveedor de Servicio, proveedor de sus equipos de puntos de venta (POS) o sistemas o de soluciones de procesamiento de pagos, Entidad asociada a su cuenta de Comercio de American Express y a cualquier otra parte a la que usted pueda facilitar Datos de Titulares de Tarjetas de conformidad con el Contrato.