AMERICAN EXPRESS

Data Security Operating Policy (DSOP)

AMERICAN EXPRESS

Resumo de Alterações da DSOP

Ícones

As atualizações importantes estão listadas na Tabela de Resumo das Alterações e também estão indicadas na *DSOP* com uma barra de alterações. As barras de alterações são linhas verticais, normalmente na margem esquerda, que identificam texto adicionado ou revisto. Somente as alterações significativas à *DSOP* com impacto potencial nos procedimentos operacionais de um comerciante são indicadas com uma barra de alterações, conforme indicado na margem esquerda.

O texto removido é destacado com um ícone de caixote do lixo colocado na margem junto a qualquer texto que tenha sido eliminado de forma significativa, incluindo secções, tabelas, parágrafos, notas e marcadores. O texto removido é referenciado no presente Resumo de Alterações utilizando a numeração de secção da publicação anterior para evitar confusões.

As linhas azuis que delimitam os parágrafos indicam informações específicas da região.

Tabela de Resumo das Alterações

As atualizações importantes estão listadas na tabela seguinte e também estão indicadas na *DSOP* com uma barra de alterações.

Secção/Subsecção	Descrição da alteração
Não há alterações nesta versão.	

Secção 1 Introdução à DSOP e aos Padrões para a Proteção

Na qualidade de líder na defesa do consumidor, a American Express assumiu há muito o compromisso de proteger os Dados do Titular do Cartão e os Dados de Autenticação Sensíveis, garantindo que são mantidos em segurança.

A existência de dados em risco tem um impacto negativo nos consumidores, Comerciantes, Fornecedores de Serviços e entidades emissoras de cartões. Um único incidente pode afetar gravemente a reputação de uma empresa e limitar a sua capacidade de desempenhar as suas atividades de forma eficaz. Combater esta ameaça implementando políticas operacionais de segurança pode ajudar a estimular a confiança do cliente, aumentar a rentabilidade e melhorar a reputação da empresa.

A American Express sabe que os nossos Comerciantes e Fornecedores de Serviços (coletivamente, **Comerciantes e Fornecedores**) partilham as mesmas preocupações e exige, no âmbito das responsabilidades dos mesmos, o cumprimento das disposições de segurança de dados constantes no Acordo de aceitação (no caso dos Comerciantes) ou de processamento (no caso dos Fornecedores de Serviços) do Cartão American Express® (cada, respetivamente, o **Acordo**), bem como da presente Política Operacional de Segurança de Dados (DSOP), que poderá sofrer alterações periodicamente. Estes requisitos são aplicáveis a todos os equipamentos, sistemas e redes (e respetivos componentes), nos quais sejam armazenados, processados ou transmitidos Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (ou uma combinação de ambos) ou Chaves de encriptação.

Os termos utilizados em maiúsculas, mas que não estão definidos, encontram-se descritos no glossário no fim da presente política.

A Política Operacional de Segurança de Dados (DSOP) é um conjunto de requisitos de política abrangentes concebidos para proteger os Dados de Conta sempre que os mesmos são armazenados, processados ou transmitidos.

A American Express exige que todos os Comerciantes e Fornecedores de Serviços estejam em conformidade com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (Payment Card Industry Data Security Standard, PCI DSS). Os Comerciantes e Fornecedores de Serviços, bem como as Partes Abrangidas têm as seguintes obrigações:

- Armazenar Dados do Titular do Cartão apenas para facilitar as Transações com Cartões American Express em conformidade com o Acordo e como requerido pelo mesmo.
- Cumprir a versão atual do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) e outros Requisitos do Payment Card Industry Security Standards Council (PCI SSC) aplicáveis ao seu processamento, armazenamento ou transmissão de Chaves de Encriptação, Dados do Titular do Cartão ou Dados de Autenticação Sensíveis o mais tardar até à data em vigor de implementação dessa versão do requisito aplicável.
- Garantir que são utilizados produtos aprovados pelo PCI aquando da implementação ou substituição de tecnologia para armazenar, processar ou transmitir dados.

Os Comerciantes e Fornecedores têm o dever de proteger todos os registos de Crédito e todos os registos de Cobrança da American Express retidos, conforme previsto no Acordo, em conformidade com as presentes disposições de segurança de dados; os Comerciantes e Fornecedores devem utilizar estes registos apenas para os fins previstos no Acordo e proteger os mesmos em conformidade. Os Comerciantes e Fornecedores são responsáveis, em termos financeiros e outros, perante a American Express por garantir o cumprimento destas disposições de segurança por parte das Partes Abrangidas (além de demonstrar a conformidade das Partes Abrangidas com a presente política na Secção 2, "Programa de Conformidade do PCI DSS (Importante Validação Periódica dos seus Sistemas)", salvo indicação em contrário na referida secção). Para mais informações sobre os padrões do PCI e sobre como cumprir os seus requisitos, consulte www.pcisecuritystandards.org.

Secção 2 Programa de Conformidade do PCI DSS (Importante Validação Periódica dos seus Sistemas)

O Comerciante ou Fornecedor tem de realizar as ações seguintes para efetuar a validação anual e a cada 90 dias junto do PCI DSS tal como descrito abaixo, do estado dos equipamentos do Comerciante ou Fornecedor e dos seus concessionários, sistemas e/ou redes (e respetivos componentes) nos quais os Dados do Titular do Cartão ou os Dados de Autenticação Sensíveis são armazenados, processados ou transmitidos.

Existem quatro ações necessárias para concluir a validação:

- Ação 1: Participar no programa de conformidade do PCI da American Express no âmbito da presente política.
- Ação 2: Compreender o Nível do Comerciante/Fornecedor de Serviços e os Requisitos da Documentação de Validação.
- Ação 3: Preencher a Documentação de Validação a enviar para a American Express.
- Ação 4: Enviar a Documentação de Validação para a American Express dentro dos prazos indicados.

Ação 1: Participar no Programa de Conformidade da American Express no âmbito da presente Política

Os Comerciantes de Nível 1, os Comerciantes de Nível 2 e todos os Fornecedores de Serviços, conforme descrito abaixo, têm de participar no Programa no âmbito da presente política. A American Express poderá requerer, a seu exclusivo critério, que Comerciantes de Nível 3 e Nível 4 específicos participem no Programa no âmbito da presente política.

Os Comerciantes e Fornecedores de Serviços com obrigatoriedade de participar no Programa devem inscrever-se no Portal fornecido pelo Administrador do Programa, selecionado pela American Express, dentro dos prazos indicados.

- Os Comerciantes e Fornecedores de Serviços têm de aceitar todos os termos e condições razoáveis associados à utilização do Portal.
- Os Comerciantes e Fornecedores de Serviços têm de designar e fornecer informações precisas para, pelo menos, um contacto de segurança de dados no Portal. As informações necessárias incluem:
  - Nome completo
  - Endereço de e-mail
  - Número de telefone
  - Endereço postal físico
- Os Comerciantes e Fornecedores de Serviços têm de fornecer informações atualizadas ou novas informações de contacto para o contacto de segurança de dados designado no Portal, quando estas informações forem alteradas.
- Os Comerciantes e Fornecedores de Serviços têm de garantir que os seus sistemas estão atualizados para permitir comunicações de serviço a partir do domínio designado do Portal.

Caso o Comerciante ou Fornecedor não forneça nem mantenha informações de contacto de segurança de dados atualizadas ou não permita as comunicações por e-mail, os nossos direitos de avaliar as taxas não serão afetados.

Ação 2: Compreender o Nível do Comerciante/Fornecedor de Serviços e os Requisitos da Documentação de Validação

Existem quatro Níveis aplicáveis aos Comerciantes e dois Níveis aplicáveis aos Fornecedores de Serviços baseados no volume de Transações do Cartão American Express dos Comerciantes ou Fornecedores.

- Para os Comerciantes, este é o volume submetido pelos seus Estabelecimentos acumulado até ao nível de conta mais alto de Comerciante da American Express.*
- Para os Fornecedores de Serviços, esta é a soma do volume submetido pelo Fornecedor de Serviços e Entidades Fornecedoras de Serviço a quem são prestados os serviços.

As Transações de Pagamentos Iniciados pelo Comprador (Buyer Initiated Payments, BIP) não são incluídas no volume de Transações com Cartão American Express para determinar o Nível do Comerciante e os requisitos de validação. Os Comerciantes ou Fornecedores de Serviços são classificados num dos Níveis de Comerciante especificados na Tabela A-1: Níveis de Comerciante e Fornecedor de Serviços.

* No caso de Franqueadores, tal inclui o volume dos seus Estabelecimentos Concessionários. Os Franqueadores que impõem aos seus Concessionários a utilização de um Sistema de Ponto de Venda (Point of Sale, POS) ou Fornecedor de Serviços especificado têm também de fornecer documentação de validação para os Concessionários afetados.

Tabela A-1: Níveis de Comerciante e Fornecedor de Serviços

Nível de Comerciante	Transações Anuais da American Express
Comerciante de Nível 1	2,5 milhões de Transações com Cartão American Express ou mais por ano; ou, por outro lado, qualquer Comerciante que a American Express considere, a seu critério, de Nível 1.
Comerciante de Nível 2	50.000 a menos de 2,5 milhões de Transações com Cartão American Express por ano.
Comerciante de Nível 3	10.000 a menos de 50.000 milhões de Transações com Cartão American Express por ano.
Comerciante de Nível 4	Menos de 10.000 Transacções com o Cartão American Express por ano.
Nível de Fornecedor de Serviços	**Transações Anuais da American Express**
Fornecedor de Serviços de Nível 1	2,5 milhões de Transações com Cartão American Express ou mais por ano; ou qualquer Fornecedor de Serviços que a American Express considere de Nível 1.
Fornecedor de Serviços de Nível 2	menos de 2,5 milhões de Transações com Cartão American Express por ano; ou qualquer Fornecedor de Serviços não considerado de Nível 1 pela American Express.

Requisitos da Documentação de Validação de Comerciantes

Os Comerciantes (não Fornecedores de Serviços) têm quatro classificações possíveis de Nível de Comerciante. Após determinar o nível do Comerciante na Tabela A-1: Níveis de Comerciante e Fornecedor de Serviços (acima), consulte a Tabela A-2: Documentação de Validação de Comerciantes para determinar os requisitos de documentação de validação.

Tabela A-2: Documentação de Validação de Comerciantes

Nível do Comerciante/ Transações Anuais da American Express	Relatório de Conformidade do Certificado de Conformidade (ROC AOC)	Questionário de Autoavaliação do Certificado de Conformidade (SAQ AOC) E Verificação Trimestral de Rede (Verificação)	Certificado do Programa de Melhoria de Tecnologias de Segurança (STEP) para Comerciantes elegíveis
Nível 1/ 2,5 milhões ou mais	Obrigatório	Não aplicável	Opcional com a aprovação da American Express (substitui o ROC)
Nível 2/ 50.000 a menos de 2,5 milhões	Opcional	SAQ AOC obrigatório (exceto se for enviado um ROC AOC); verificação obrigatória com determinados tipos SAQ	Opcional com aprovação da American Express* (substitui a verificação SAQ e de rede ou ROC)
Nível 3**/ 10.000 a menos de 50.000	Opcional	SAQ AOC opcional (obrigatório se solicitado pela American Express); verificação obrigatória com determinados tipos SAQ	Opcional com aprovação da American Express* (substitui a verificação SAQ e de rede ou ROC)
Nível 4**/ Menos de 10.000	Opcional	SAQ AOC opcional (obrigatório se solicitado pela American Express); verificação obrigatória com determinados tipos SAQ	Opcional com aprovação da American Express* (substitui a verificação SAQ e de rede ou ROC)

* **Nota:** a equipa do PCI da American Express analisará o pedido e a elegibilidade e confirmará se é elegível para o Programa STEP. Contacte o seu Gestor de Clientes e/ou utilize o endereço AXPPCIComplianceProgram@aexp.com para verificar a elegibilidade.

**De forma a evitar qualquer dúvida, os Comerciantes de Nível 3 e Nível 4 não têm de submeter Documentação de Validação, exceto se requerido a critério da American Express, contudo, têm de cumprir, sendo responsáveis em todas as restantes disposições, a presente Política Operacional de Segurança de Dados.

A American Express reserva o direito de verificar a integridade, a exatidão e a adequação da Documentação de Validação do PCI. A American Express pode exigir que o Comerciante ou Fornecedor forneça documentos de apoio adicionais para fins de avaliação, como forma de fundamentar este objetivo. Além disso, a American Express tem o direito de exigir que o Comerciante ou Fornecedor contrate um Assessor de Segurança Qualificado (QSA) ou Investigador Forense (PFI) do PCI aprovado pelo Security Standards Council.

Requisitos da Documentação de Validação de Fornecedores de Serviços

Os Fornecedores de Serviços (não Comerciantes) têm duas classificações possíveis de Nível. Após determinar o Nível do Fornecedor de Serviços na Tabela A-1: Níveis de Comerciante e Fornecedor de Serviços (acima), consulte a Tabela A-3: Documentação de Validação de Fornecedores de Serviços para determinar os requisitos da documentação de validação.

Os Fornecedores de Serviços não são elegíveis para o Programa STEP.

Tabela A-3: Documentação de Validação de Fornecedores de Serviços

Nível	Documentação de Validação	Requisito
1	Relatório Anual de Conformidade do Certificado de Conformidade (ROC AOC)	Obrigatório
2	SAQ D Anual (Fornecedor de Serviços) e Verificação Trimestral de Rede ou Relatório Anual de Conformidade do Certificado de Conformidade (ROC AOC), se pretendido	Obrigatório

É recomendado que os Fornecedores de Serviços cumpram também a Validação Suplementar de Entidades Designadas do PCI.

Programa de Melhoria de Tecnologias de Segurança (STEP)

Os Comerciantes em conformidade com o PCI DSS podem, a critério da American Express, ser elegíveis para o Programa de Melhoria de Tecnologias de Segurança (Security Technology Enhancement Programme, STEP) da American Express se implementarem determinadas tecnologias de segurança adicional em todo o seu ambiente de processamento de Cartões. O STEP é aplicável apenas se o Comerciante não tiver tido um Incidente de Dados nos 12 meses anteriores e se 75% de todas as Transações por Cartão do Comerciante forem efetuadas utilizando uma combinação das seguintes opções de melhoria de segurança:

- **EMV, EMV Contactless ou Carteira Digital** – num Dispositivo Eletrónico Compatível ativo com uma aprovação/certificação EMVCo (www.emvco.com) válida e atualizada e com a capacidade de processar Transações com Cartões Eletrónicos compatíveis com AEIPS. (Os Comerciantes dos Estados Unidos têm de incluir cartões Contactless)
- **Encriptação Ponto a Ponto (Point-to-Point Encryption, P2PE)** – comunicada ao processador do Comerciante utilizando um sistema de Encriptação Ponto a Ponto aprovado pelo PCI SSC ou pelo QSA
- **Utilização de tokens** – a solução de utilização de tokens implementada tem de:
  - cumprir as especificações da EMVCo,
  - ser protegida, processada, armazenada, transmitida e inteiramente administrada por um fornecedor de serviços de terceiros em conformidade com o PCI, e
  - o Token não pode ser invertido para revelar Números de Conta Principal (Primary Account Number, PAN) sem máscara ao Comerciante.

Os Comerciantes elegíveis para o Programa STEP apresentam requisitos reduzidos de Documentação de Validação do PCI, conforme descrito na Ação 3: Preencher a Documentação de Validação a enviar para a American Express abaixo.

Ação 3: Preencher a Documentação de Validação a enviar para a American Express

Os seguintes documentos são necessários para diferentes níveis de Comerciante e de Fornecedor de Serviços, conforme indicado acima na Tabela A-2: Documentação de Validação de Comerciantes e Tabela A-3: Documentação de Validação de Fornecedores de Serviços.

O Comerciante ou Fornecedor tem de fornecer o Certificado de Conformidade (AOC) para o tipo de avaliação aplicável. O AOC é uma declaração do estatuto de conformidade do Comerciante ou Fornecedor e, como tal,

deve ser assinada e datada pelo nível de liderança apropriado dentro da organização do Comerciante ou Fornecedor.

Além do AOC, a American Express pode exigir ao Comerciante ou Fornecedor uma cópia da avaliação minuciosa e, a nosso critério, documentos de apoio adicionais que demonstrem a conformidade com os requisitos do PCI DSS. Esta Documentação de Validação é preenchida a cargo do Comerciante ou Fornecedor.

Relatório de Conformidade do Certificado de Conformidade (ROC AOC) - (Requisito Anual) – O Relatório de Conformidade documenta os resultados de uma análise local e detalhada do seu equipamento, sistemas e redes (e respetivos componentes) nos quais os Dados do Titular do Cartão ou os Dados de Autenticação Sensíveis (ou ambos) são armazenados, processados ou transmitidos. Existem duas versões: uma para Comerciantes e outra para Fornecedores de Serviços. O Relatório de Conformidade tem de ser realizado por:

- um QSA, ou
- um Assessor de Segurança Interna (ISA) e certificado pelo diretor executivo, diretor financeiro, diretor da segurança de informação ou responsável principal do Comerciante ou Fornecedor

O ROC AOC deve ser assinado e datado por um QSA ou ISA e pelo nível de liderança autorizado dentro na organização do Comerciante ou Fornecedor e enviado à American Express, pelo menos, uma vez por ano.

Questionário de Autoavaliação do Certificado de Conformidade (SAQ AOC) - (Requisito Anual) – Os Questionários de Autoavaliação permitem a autoanálise do seu equipamento, sistemas e redes (e respetivos componentes) nos quais os Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (ou ambos) são armazenados, processados ou transmitidos. Existem múltiplas versões do SAQ. O Comerciante ou Fornecedor de Serviços deverá selecionar uma ou mais versões com base no Ambiente de Dados do Titular do Cartão.

O SAQ pode ser preenchido pelo pessoal da Empresa do Comerciante ou Fornecedor qualificado para responder às perguntas de forma precisa e completa ou o Comerciante ou Fornecedor pode contratar um QSA para auxiliar no preenchimento. O SAQ AOC deve ser assinado e datado pelo nível de liderança autorizado dentro na organização do Comerciante ou Fornecedor e enviado à American Express, pelo menos, uma vez por ano.

Resumo de Vulnerabilidade da Rede Externa do Assessor de Verificação Aprovado - (Verificação do ASV) – (Requisito de 90 dias) - Uma verificação de vulnerabilidade externa é um teste remoto para ajudar a identificar potenciais falhas, vulnerabilidades e erros de configuração dos componentes do Ambiente de Dados do Titular do Cartão (por exemplo, websites, aplicações, servidores web, servidores de correio eletrónico, domínios em contacto com o público ou anfitriões).

A Verificação do ASV tem de ser realizada por um Fornecedor de Verificação Aprovado (Approved Scanning Vendor, ASV).

Se exigido pelo SAQ, o Relatório de Análise do ASV do Certificado de Conformidade de Verificação (Attestation of Scan Compliance, AOSC) ou o resumo executivo incluindo uma contagem dos alvos verificados, a certificação de que os resultados satisfazem os procedimentos de verificação do PCI DSS, e o estado de conformidade têm de ser enviados à American Express, pelo menos, uma vez a cada 90 dias.

Ao enviar um ROC AOC ou STEP, ao Comerciante ou Fornecedor de Serviços não é exigida a entrega de um resumo executivo AOSC ou de Verificação do ASV, a menos que especificamente solicitado. De forma a evitar qualquer dúvida, as Verificações são obrigatórias se solicitadas pelo SAQ aplicável.

Documentação de Validação do Certificado STEP (STEP) - (Requisito Anual) – O STEP está disponível apenas para Comerciantes que cumpram os critérios indicados acima na Ação 2: Compreender o Nível do Comerciante/ Fornecedor de Serviços e os Requisitos da Documentação de Validação. Se a empresa do Comerciante ou Fornecedor reunir as condições necessárias, o Comerciante ou Fornecedor tem de preencher e enviar anualmente o formulário do Certificado STEP à American Express. O formulário do Certificado STEP está disponível para transferência através do Portal. O Comerciante ou Fornecedor pode ainda contactar o seu Gestor de Clientes ou escrever à American Express utilizando o seguinte endereço: AXPPCIComplianceProgram@aexp.com.

Não Conformidade com o PCI DSS – (Requisito Anual, 90 Dias e/ou Ad Hoc) – Se o Comerciante ou Fornecedor não cumprir todos os requisitos do PCI DSS, terá de enviar um Resumo da Ferramenta de

Abordagem Prioritária do PCI (disponível para transferência através do website do Security Standards Council do PCI).

O Resumo da Ferramenta de Abordagem Prioritária do PCI deve indicar uma data de conclusão de todas as correções que não exceda os doze (12) meses após a data de conclusão para o cumprimento dos requisitos. O Comerciante ou Fornecedor deve fornecer à American Express atualizações periódicas relativas ao seu progresso no sentido de efetuar as correções necessárias ao Estado de Não Conformidade do Comerciante ou Fornecedor (Comerciantes de Nível 1, 2, 3 e 4; todos os Fornecedores de Serviços). As ações de correção necessárias para garantir a conformidade com o PCI DSS devem ser realizadas a cargo do Comerciante ou Fornecedor.

A American Express não irá impor taxas de não conformidade antes da data de conclusão de todas as correções. Segundo a Tabela A-4: Taxa de Não Conformidade, o Comerciante ou Fornecedor permanece responsável perante a American Express por todas as obrigações de indemnização decorrentes de um Incidente de Dados e está sujeito a todas as disposições da presente política.

A American Express, a seu exclusivo critério, reserva o direito de impor taxas de não conformidade se:

- não foi enviado um Modelo de Abordagem Prioritária do PCI em conformidade com os requisitos indicados na presente secção,
- as etapas de correção delineadas no Modelo de Abordagem Prioritária do PCI para o Estado de Não Conformidade não foram cumpridas,
- não foram cumpridos os requisitos do Modelo de Abordagem Prioritária do PCI para o Estado de Não Conformidade, ou
- a documentação de conformidade obrigatória não foi fornecida à American Express dentro do prazo aplicável ou mediante pedido.

Os Comerciantes/Fornecedores de Serviços que não cumpram os requisitos especificados na Ação 2: Compreender o Nível do Comerciante/Fornecedor de Serviços e os Requisitos da Documentação de Validação, podem estar sujeitos a taxas, conforme indicado na Ação 4: Enviar a Documentação de Validação para a American Express.

Para que não subsistam dúvidas, os Comerciantes que não cumprirem os requisitos do PCI DSS não são elegíveis para o Programa STEP.

Ação 4: Enviar a Documentação de Validação para a American Express

Todos os Comerciantes e Fornecedores de Serviços, cuja participação no Programa é exigida, têm de enviar a Documentação de Validação assinalada como "obrigatória" nas tabelas da Ação 2: Compreender o Nível do Comerciante/Fornecedor de Serviços e os Requisitos da Documentação de Validação à American Express até ao fim do prazo aplicável.

O Comerciante ou Fornecedor tem de enviar a Documentação de Validação à American Express utilizando o Portal fornecido pelo Administrador do Programa selecionado pela American Express. Ao enviar a Documentação de Validação, o Comerciante ou Fornecedor declara e garante à American Express que as seguintes informações são verdadeiras (dentro das suas possibilidades):

- A avaliação é exaustiva e rigorosa;
- O estado do PCI DSS está representado de forma precisa na data da conclusão, independentemente de estar a enviar o Certificado de Conformidade (AOC) ou um Resumo da Ferramenta de Abordagem Prioritária (PAT) do PCI por não conformidade;
- O Comerciante ou Fornecedor está autorizado a divulgar as informações aí contidas e está a fornecer a Documentação de Validação à American Express sem violar os direitos de qualquer outra parte.

Taxas de Não Conformidade e Cessação do Acordo

A American Express tem o direito de cobrar taxas de não conformidade e cessar o Acordo se o Comerciante ou Fornecedor não cumprir estes requisitos ou não fornecer à American Express a documentação de validação obrigatória até ao fim do prazo aplicável. A American Express irá tentar notificar o contacto de segurança de dados relativamente ao prazo aplicável para cada período de comunicação anual e trimestral.

Tabela A-4: Taxa de Não Conformidade

Descrição*	Comerciante de Nível 1 ou Fornecedor de Serviços de Nível 1	Comerciante de Nível 2 ou Fornecedor de Serviços de Nível 2	Comerciante de Nível 3 ou Nível 4
Será ponderada uma taxa de não conformidade se a documentação de validação não for recebida até ao primeiro prazo.	$25.000 USD	$5000 USD	$50 USD
Será ponderada uma taxa adicional de não conformidade se a documentação de validação não for recebida até ao segundo prazo.	$35.000 USD	$10.000 USD	$100 USD
Será ponderada uma taxa adicional de não conformidade se a documentação de validação não for recebida até ao terceiro prazo. **NOTA:** as taxas de não conformidade vão continuar a ser aplicadas até que a documentação de validação seja enviada.	$45.000 USD	$15.000 USD	$250 USD

* As Taxas de Não Conformidade serão avaliadas em equivalentes na Moeda Local.

* Não aplicável na Argentina.

Se obrigações da documentação de conformidade do PCI DSS não forem cumpridas, a American Express tem o direito de impor as taxas de não conformidade cumulativamente, reter pagamentos e/ou rescindir o Acordo.

Secção 3 Obrigações de Gestão de Incidentes de Dados

Os Comerciantes e Fornecedores têm de notificar de imediato a American Express, sem exceder o prazo máximo de setenta e duas (72) horas, após a deteção de um Incidente de Dados.

Para notificar a American Express, contacte a equipa do Programa de Resposta a Incidentes da American Express (Enterprise Incident Response Programme, *EIRP*) através dos números gratuitos 1.888.732.3750 ou 1.602.537.3021, ou enviando um e-mail para EIRP@aexp.com. Os Comerciantes e Fornecedores têm de designar uma pessoa de contacto para esse Incidente de Dados. Além disso:

- O Comerciante ou Fornecedor têm de realizar uma investigação minuciosa de cada Incidente de Dados e fornecer prontamente à American Express todos os Números dos Cartões Comprometidos. A American Express reserva o direito de realizar a sua própria análise interna para identificar os dados envolvidos no Incidente de Dados.

No caso de Incidentes de Dados que envolvam menos de 10.000 Números de Cartão únicos, deve ser fornecido um resumo da investigação à American Express no prazo de dez (10) dias úteis após a sua conclusão.

- Os resumos de investigações devem incluir as seguintes informações: resumo do incidente, descrição do(s) ambiente(s) afetado(s), cronologia dos eventos, datas-chave, detalhes do impacto e da exposição dos dados, ações de contenção e correção e atestado de que não há indicação de que outros dados da American Express estejam em risco.

No caso de Incidentes de Dados que envolvam 10.000 ou mais Números de Cartão únicos, a investigação terá de ser realizada por um PFI de PCI no prazo de cinco (5) dias após a descoberta do Incidente de Dados.

- O relatório original de investigação forense terá de ser fornecido à American Express, no prazo de dez (10) dias úteis após a sua conclusão.
- Os relatórios de investigação forense têm de ser concluídos utilizando o Modelo do Relatório Final de Incidentes Forenses atual disponível no PCI. Este relatório tem de incluir avaliações forenses, relatórios sobre conformidade, bem como todas as restantes informações relacionadas com o Incidente de Dados; identificar a causa do Incidente de Dados; confirmar se o Comerciante ou Fornecedor estava ou não em conformidade com o PCI DSS na data do Incidente de Dados; e verificar a sua capacidade de impedir futuros Incidentes de Dados, mediante (i) o fornecimento de um plano para remediar todas as deficiências em relação ao estipulado pelo PCI DSS e (ii) a participação no programa de conformidade da American Express (tal como descrito abaixo). A pedido da American Express, o Comerciante ou Fornecedor facultará a validação de um Assessor de Segurança Qualificado (Qualified Security Assessor, QSA) em como as deficiências foram remediadas.

Não obstante os parágrafos anteriores desta Secção 3, "Obrigações de Gestão de Incidentes de Dados":

- A American Express pode, a seu exclusivo critério, exigir que o Comerciante ou Fornecedor contrate um PFI para conduzir uma investigação de um Incidente de Dados para Incidentes de Dados que envolvam menos de 10.000 Números de Cartã oúnicos ou se tiverem ocorrido vários incidentes num período de 12 meses. Qualquer investigação deste tipo tem de cumprir os requisitos acima estabelecidos na presente Subsecção 3, "Obrigações de Gestão de Incidentes de Dados" e tem de ser concluída dentro do prazo exigido pela American Express.
- A American Express pode, a seu exclusivo critério, contratar separadamente um PFI para conduzir uma investigação de qualquer Incidente de Dados e pode cobrar-lhe o custo de tal investigação.

O Comerciante ou Fornecedor deve avaliar o Incidente de Dados ao abrigo das leis de notificação de incumprimento de dados aplicáveis a nível mundial e, se necessário, notificar os reguladores aplicáveis e os Clientes de Cartões afetados, de acordo com essas leis de notificação de violação de dados. Se o Comerciante ou Fornecedor determinar que o seu Fornecedor de Serviços ou outra entidade é responsável pela comunicação do Incidente de Dados, deve informar esse Fornecedor de Serviços ou entidade do seu dever de avaliar as suas obrigações de comunicação ao abrigo das leis de notificação de violação de dados aplicáveis. O Comerciante ou Fornecedor concorda em obter a aprovação por escrito da American Express antes de fazer referência ou mencionar a American Express em quaisquer comunicações aos Clientes de Cartões sobre o Incidente de Dados. O Comerciante ou Fornecedor concorda em colaborar com a American Express para fornecer detalhes e retificar quaisquer questões decorrentes do Incidente de Dados, incluindo fornecer (e obter quaisquer renúncias

necessárias para fornecer) à American Express todas as informações relevantes para verificar a sua capacidade de prevenir futuros Incidentes de Dados de uma forma consistente com o Acordo.

Não obstante qualquer obrigação de confidencialidade em contrário no Acordo, a American Express tem o direito de divulgar informação sobre qualquer Incidente de Dados aos Clientes de Cartões da American Express, bem como a Entidades Emissoras, outros participantes da rede da American Express e o público geral, conforme requerido pela Lei Aplicável; por ordem judicial, administrativa ou regulamentar, decreto, intimação, pedido ou outro processo; para mitigar o risco de fraude ou outros danos; ou, de outra forma, até à extensão adequada para operar a Rede American Express.

Como proceder em caso de um Incidente de Dados?

Siga os passos que se seguem, caso tenha identificado um Incidente de Dados na sua empresa.

1.º passo:

Preencha o Formulário de Notificação Inicial relativa a Incidentes de Dados do Comerciante e envie o mesmo para o endereço EIRP@aexp.com no prazo de 72 horas após ser detetado o Incidente de Dados.

2.º passo:

Leve a cabo uma investigação minuciosa; para tal, poderá ser necessário contratar um Investigador Forense do Payment Card Industry (PCI).

3.º passo:

Disponibilize-nos de imediato todos os números de Cartões American Express® comprometidos.

4.º passo:

Colabore connosco para ajudar a resolver quaisquer questões decorrentes do Incidente de Dados.

Consulte a Secção 3, "Obrigações de Gestão de Incidentes de Dados" para obter mais informações sobre as Obrigações de Gestão de Incidentes de Dados.

Dúvidas?

EUA: (888) 732-3750 (chamada gratuita)

Internacional: +1 (602) 537-3021

EIRP@aexp.com

Secção 4 Obrigações de Indemnização para um Incidente de Dados

As obrigações de indemnização dos Comerciantes e Fornecedores para com a American Express no âmbito do Acordo para Incidentes de Dados serão determinadas, sem renúncia de quaisquer outros direitos e reparações da American Express, conforme o estipulado na presente Secção 4, "Obrigações de Indemnização para um Incidente de Dados". Para além das suas obrigações de indemnização (se existirem), o Comerciante ou Fornecedor pode estar sujeito a uma taxa de não conformidade por Incidente de Dados, tal como descrito nesta Secção 4, "Obrigações de Indemnização para um Incidente de Dados".

O Comerciante ou Fornecedor compensará a American Express no valor de $5 USD por número de conta, para Incidentes de Dados que envolvam:

- 10.000 ou mais Números de Cartão American Express com um dos seguintes:
  - Dados de Autenticação Sensíveis, ou
  - Prazo de Validade

No entanto, a American Express não irá pedir ao Comerciante ou Fornecedor uma indemnização por um Incidente de Dados que envolva:

- menos de 10.000 Números de Cartão American Express, ou
- mais de 10.000 Números de Cartão American Express, se cumprir as seguintes condições:
  - o Comerciante ou Fornecedor tiver notificado a American Express do incidente de dados de acordo com a Secção 3, "Obrigações de Gestão de Incidentes de Dados",
  - o Comerciante ou Fornecedor estava em conformidade com o PCI DSS na data do Incidente de Dados (conforme determinado pela investigação do PFI do Incidente de Dados), e
  - o Incidente de Dados não foi causado por conduta indevida do Comerciante ou Fornecedor nem das suas Partes Abrangidas.

Não obstante os parágrafos anteriores desta Secção 4, "Obrigações de Indemnização para um Incidente de Dados", para qualquer Incidente de Dados, independentemente da quantidade de Números de Cartão American Express, o Comerciante ou Fornecedor deverá pagar à American Express uma taxa de não conformidade de Incidente de Dados não superior a $100.000 USD por Incidente de Dados (conforme determinado pela American Express a seu exclusivo critério), no caso de não cumprir qualquer uma das suas obrigações estabelecidas na Secção 3, "Obrigações de Gestão de Incidentes de Dados". De forma a evitar qualquer dúvida, a taxa total de não conformidade de Incidente de Dados avaliada para qualquer Incidente de Dados não deve exceder $100.000 USD.

A American Express irá excluir dos seus cálculos qualquer número de conta de Cartão American Express envolvido noutro Incidente de Dados com números de conta de Cartão American Express com Dados de Autenticação Sensíveis, desde que a American Express tenha sido notificada do outro Incidente de Dados no prazo de doze (12) meses antes da Data de Notificação. Todos os cálculos realizados pela American Express segundo esta metodologia são finais.

A American Express poderá cobrar ao Comerciante ou Fornecedor o montante total das suas obrigações de indemnização por Incidentes de Dados ou deduzir o montante dos pagamentos da American Express (ou debitar da Conta Bancária do Comerciante ou Fornecedor, respetivamente) nos termos do Acordo.

As obrigações de indemnização do Comerciante ou Fornecedor por Incidentes de Dados nos presentes termos não serão consideradas danos incidentais, indiretos, especulativos, consequentes, especiais, punitivos ou exemplares no âmbito do Acordo; desde que tais obrigações não incluam danos relacionados com ou de natureza de perda de lucros ou receitas, perda de credibilidade ou perda de oportunidades de negócio.

A seu critério exclusivo, a American Express pode reduzir a obrigação de indemnização para os Comerciantes exclusivamente para Incidentes de Dados que cumpram todos os critérios seguintes:

- As Tecnologias de Mitigação de Riscos aplicáveis foram utilizadas antes do Incidente de Dados e estavam em utilização durante todo o Período do Evento de Incidente de Dados,
- Foi realizada uma investigação minuciosa em conformidade com o programa do PFI (salvo acordo escrito prévio em contrário),

- O relatório forense indica de forma clara as Tecnologias de Mitigação de Riscos que foram utilizadas para processar, armazenar e/ou transmitir os dados na data do Incidente de Dados, e
- O Comerciante ou Fornecedor não armazena (e não armazenou durante o Período do Evento de Incidente de Dados) Dados de Autenticação Sensíveis ou quaisquer Dados do Titular do Cartão que não tenham sido tornados ilegíveis.

Quanto existe uma redução de indemnização disponível, a redução da obrigação de indemnização do Comerciante ou Fornecedor é determinada do seguinte modo:

Tabela A-5: Critérios Requeridos para a Redução da Obrigação de Indemnização

Redução da Obrigação de Indemnização	Critérios requeridos
Redução Padrão: 50%	>75% do total das Transações processadas em Dispositivos Eletrónicos Compatíveis[1] OU
	Tecnologia de Mitigação de Riscos em utilização em >75% das localizações do Comerciante[2]
Redução Maximizada: 75% a 100%	>75% de todas as Transações processadas em Dispositivos Eletrónicos Compatíveis[1] E outra Tecnologia de Mitigação de Riscos em utilização em >75% das localizações do Comerciante[2]

[1] Conforme determinado pela análise interna da American Express

[2] Conforme determinado pela investigação do PFI

- A Redução Maximizada (75% a 100%) será determinada com base no menor valor de percentagem de Transações utilizando Dispositivos Eletrónicos Compatíveis E localizações do Comerciante que utilizam outra Tecnologia de Mitigação de Riscos. Os exemplos na Tabela A-6: Redução Maximizada da Obrigação de Indemnização ilustram o cálculo da redução da indemnização.
- Para ser considerada uma Tecnologia de Mitigação de Riscos, o Comerciante ou Fornecedor tem de demonstrar a utilização efetiva da tecnologia de acordo com a sua conceção e finalidade pretendida.
- A percentagem de localizações que utilizam uma Tecnologia de Mitigação de Riscos é determinada pela investigação do PFI.
- A redução da obrigação de indemnização não é aplicável a quaisquer taxas de não conformidade a pagar em relação ao Incidente de Dados.

Tabela A-6: Redução Maximizada da Obrigação de Indemnização

Ex.	Tecnologias de Mitigação de Riscos em utilização	Elegível	Redução
1	• 80% das Transações em Dispositivos Eletrónicos Compatíveis • 0% das localizações utilizam outras Tecnologias de Mitigação de Riscos	Não	50%: Redução Padrão (menos de 75% de utilização de Tecnologias de Mitigação de Riscos não é elegível para Redução Maximizada)[1]
2	• 80% das Transações em Dispositivos Eletrónicos Compatíveis • 77% das localizações utilizam outras Tecnologias de Mitigação de Riscos	Sim	77%: Redução Maximizada (baseada em 77% de utilização de Tecnologia de Mitigação de Riscos)
3	• 93% das Transações em Dispositivos Eletrónicos Compatíveis • 100% das localizações utilizam outras Tecnologias de Mitigação de Riscos	Sim	93%: Redução Maximizada (baseada em 93% das Transações em Dispositivos Eletrónicos Compatíveis)
4	• 40% das Transações em Dispositivos Eletrónicos Compatíveis • 90% das localizações utilizam outras Tecnologias de Mitigação de Riscos	Não	50%: Redução Padrão (menos de 75% de Transações em Dispositivos Eletrónicos Compatíveis não é elegível para Redução Maximizada)

[1] Um Incidente de Dados envolvendo 10.000 Contas de Cartão American Express, a uma taxa de $5 USD por número de conta (10.000 x $5 = $50.000 USD) pode ser elegível para uma redução de 50%, reduzindo as Obrigações de Indemnização de $50.000 USD para $25.000 USD, excluindo quaisquer taxas de não conformidade.

Secção 5 Programa de Análise Direcionada (Targeted Analysis Programme, TAP)

Os comprometimentos de dados do Titular do Cartão podem ser causados por falhas de segurança de dados no seu Ambiente de Dados do Titular do Cartão (Cardholder Data Environment, CDE).

Exemplos do comprometimento dos Dados do Titular do Cartão incluem, mas não estão limitados a:

- **Ponto de Compra Comum (Common Point of Purchase, CPP):** os Titulares do Cartão American Express relatam Transações fraudulentas nas suas contas de Cartão e são identificadas e determinadas como originadas de compras nos seus Estabelecimentos.
- **Dados do Cartão encontrados:** dados do Cartão American Express e Dados do Titular do Cartão encontrados na rede mundial de computadores vinculados a Transações nos seus Estabelecimentos.
- **Malware suspeito:** a American Express suspeita que o Comerciantes ou Fornecedor está a utilizar um software infetado ou vulnerável a código malicioso.

O TAP foi criado para identificar potenciais comprometimentos dos Dados do Titular do Cartão.

Os Comerciantes e Fornecedores de Serviços, bem como as Partes Abrangidas, têm de cumprir os seguintes requisitos mediante notificação da American Express sobre um possível comprometimento de Dados do Titular do Cartão.

- Tem de rever imediatamente o seu CDE para detetar falhas de segurança de dados e corrigir quaisquer descobertas.
  - Tem de fazer com que o(s) seu(s) fornecedor(es) terceirizado(s) conduzam uma investigação completa do seu CDE, caso seja terceirizado.
- Tem de fornecer um resumo das ações tomadas ou planeadas dos seus esforços de revisão, avaliação e/ou correção mediante notificação da American Express.
- O Comerciante ou Fornecedor de Serviços tem de fornecer documentos de validação do PCI DSS atualizados de acordo com a Secção 2, "Programa de Conformidade do PCI DSS (Importante Validação Periódica dos seus Sistemas)".
- Se aplicável, os Comerciantes e Fornecedores de Serviços têm de contratar um PFI do PCI qualificado para examinar o respetivo CDE, se estes ou a Parte Abrangida:
  - Não conseguirem resolver o comprometimento dos dados do Titular do Cartão num período de tempo razoável, conforme determinado pela American Express, ou
  - Confirmarem que ocorreu um Incidente de Dados e cumprirem os requisitos definidos na Secção 3, "Obrigações de Gestão de Incidentes de Dados".

Tabela A-7: Taxa de Não Conformidade do TAP

Descrição	Comerciante de Nível 1 ou Fornecedor de Serviços de Nível 1	Comerciante de Nível 2 ou Fornecedor de Serviços de Nível 2	Comerciante de Nível 3 ou Nível 4
Taxa de não conformidade pode ser avaliada quando as obrigações do TAP não são satisfeitas até ao primeiro prazo.	$25.000 USD	$5000 USD	$1000 USD
Taxa de não conformidade pode ser avaliada quando as obrigações do TAP não são satisfeitas até ao segundo prazo.	$35.000 USD	$10.000 USD	$2500 USD

Tabela A-7: Taxa de Não Conformidade do TAP (Continuação)

Descrição	Comerciante de Nível 1 ou Fornecedor de Serviços de Nível 1	Comerciante de Nível 2 ou Fornecedor de Serviços de Nível 2	Comerciante de Nível 3 ou Nível 4
Taxa de não conformidade pode ser avaliada quando as obrigações do TAP não são satisfeitas até ao terceiro prazo. **NOTA:** *as taxas de não conformidade podem continuar a ser aplicadas até que as obrigações sejam cumpridas ou o TAP seja resolvido.*	$45.000 USD	$15.000 USD	$5000 USD

Se as obrigações do TAP não forem cumpridas, a American Express tem o direito de impor as Taxas de não conformidade cumulativamente, reter pagamentos e/ou rescindir o Acordo.

Secção 6 Confidencialidade

A American Express tomará medidas razoáveis para manter (e fazer com que os seus agentes e subcontratantes, incluindo o fornecedor do Portal, mantenham) os relatórios do Comerciante ou Fornecedor relativos à conformidade, incluindo a Documentação de Validação, confidenciais e não divulgar a Documentação de Validação a quaisquer entidades terceiras (exceto às afiliadas, agentes, representantes, Fornecedores de Serviços e subcontratantes da American Express) durante um período de três anos a partir da data de receção, exceto se esta obrigação de confidencialidade não for aplicável a Documentação de Validação que:

a. já seja do conhecimento da American Express antes da sua divulgação;

b. está ou foi disponibilizada publicamente pela American Express por outro meio que não em incumprimento do presente parágrafo;

c. foi legitimamente recebida da parte de uma entidade terceira, pela American Express, sem qualquer obrigação de confidencialidade;

d. está a ser desenvolvida de forma independente pela American Express; ou

e. tem de ser divulgada devido a uma ordem judicial, serviço administrativo ou autoridade governamental, ou devido a uma lei, regra ou outro processo administrativo ou judicial, bem como devido a um inquérito ou investigação formal ou informal levados a cabo por um organismo ou autoridade governamental (incluindo uma entidade reguladora, de inspeção, avaliação ou uma força de segurança).

Secção 7 Limitação de Responsabilidade

A AMERICAN EXPRESS DECLINA PELO PRESENTE DOCUMENTO TODAS E QUAISQUER REPRESENTAÇÕES, GARANTIAS E RESPONSABILIDADES RELATIVAS A ESTA POLÍTICA OPERACIONAL DE SEGURANÇA DE DADOS, AO PCI DSS, A ESPECIFICAÇÕES EMV E A DESIGNAÇÃO E EXECUÇÃO DE QSA, ASV OU PFI (OU A QUALQUER UM DELES), SEJAM ELAS EXPRESSAS, IMPLÍCITAS, REGULAMENTARES OU QUE, DE OUTRA FORMA, INCLUAM QUALQUER GARANTIA DE COMERCIALIZAÇÃO OU ADEQUAÇÃO PARA UMA DETERMINADA FINALIDADE. AO ABRIGO DESTA POLÍTICA, AS ENTIDADES EMISSORAS DE CARTÕES AMERICAN EXPRESS NÃO SÃO TERCEIROS BENEFICIÁRIOS.

Secção 8 Glossário

Apenas para efeitos da presente *Política Operacional de Segurança de Dados*, aplicam-se as seguintes definições:

Acordo refere-se às Disposições Gerais, aos Regulamentos do Comerciante e a quaisquer calendários e documentos que os acompanham, coletivamente (por vezes referidos nos nossos materiais como o Acordo de Aceitação de Cartão).

Ambiente de Dados do Titular do Cartão (Cardholder Data Environment, CDE) refere-se às pessoas, processos e tecnologia que armazena, processa ou transmite dados do titular do cartão ou dados de autenticação sensíveis.

Aplicação de Pagamento tem o significado que lhe é atribuído no presente Glossário de Termos para o Padrão de Software Seguro e o Padrão de Ciclo de Vida de Software Seguro, que está disponível em www.pcisecuritystandards.org.

Aprovado pelo PCI significa que um Dispositivo com Introdução de PIN ou uma Aplicação de Pagamento (ou ambos) são apresentados à data da implementação na lista de empresas e fornecedores aprovados mantida pelo PCI Security Standards Council, LLC, que está disponível em www.pcisecuritystandards.org.

Assessor de Segurança Qualificado (Qualified Security Assessor, QSA), refere-se a uma entidade qualificada pelo Payment Card Industry Security Standards Council, LLC com o objetivo de validar o cumprimento dos requisitos do PCI DSS.

Cartão American Express, ou **Cartão**, refere-se a qualquer cartão, dispositivo de acesso a contas ou dispositivo de pagamento, ou qualquer serviço com o nome, logótipo, marca comercial, marca de serviço, designação comercial da American Express ou de uma afiliada, bem como outra conceção ou designação proprietária emitida através de uma entidade emissora ou número de conta de cartão.

Cartão Eletrónico refere-se a um Cartão que contém um Chip e que pode requerer um PIN como meio de verificação da identidade do Cliente do Cartão ou a informação de conta contida no Chip, ou ambos (por vezes designado nos nossos documentos como "cartão inteligente", "cartão EMV", "cartão de circuitos integrados" ou "ICC" [integrated circuit card]).

Certificado de Conformidade (Attestation of Compliance, AOC), refere-se a uma declaração do estado de conformidade do PCI DSS, no formulário fornecido pelo Payment Card Industry Security Standards Council, LLC.

Certificado de Conformidade de Verificação (Attestation of Scan Compliance, AOSC), refere-se a uma declaração do estado de conformidade com o PCI DSS com base numa verificação da rede, no formulário fornecido pelo Payment Card Industry Security Standards Council, LLC.

Chave de Encriptação (Chave de encriptação da American Express) refere-se a todas as chaves utilizadas no processamento, criação, carregamento e/ou proteção dos Dados de Conta. Tal inclui, mas não se limita, ao seguinte:

- Chaves de Encriptação Principais: Chaves Mestras de Zona (Zone Master Keys, ZMK) e Chaves de Pins de Zona (Zone Pin Keys, ZPK)
- Chaves Mestras utilizadas em dispositivos criptográficos seguros: Chaves Mestras Locais (Local Master Keys, LMK)
- Chaves de Código de Segurança do Cartão (Card Security Code Keys, CSCK)
- Chaves PIN: Chaves de Derivação Base (Base Derivation Keys, BDK), Chaves de Encriptação por PIN (PIN Encryption Keys, PEK) e ZPK

Chip refere-se a um microchip integrado inserido num Cartão que contém informações do Cliente do Cartão e da conta.

Cliente do Cartão refere-se a um indivíduo ou entidade (i) que assinou um contrato para uma conta de Cartão com uma entidade emissora ou (ii) cujo nome é apresentado no Cartão.

Cobrança refere-se a um pagamento ou compra efetuados com um Cartão.

Comerciante refere-se ao Comerciante ou a todas as suas afiliadas que aceitem Cartões American Express ao abrigo de um Acordo com a American Express ou com as suas afiliadas.

Comerciante de Nível 1 refere-se a um Comerciante com 2,5 milhões de Transações com Cartão American Express ou mais por ano; ou qualquer Comerciante que a American Express considere de Nível 1.

Comerciante de Nível 2 refere-se a um Comerciante com 50.000 a menos de 2,5 milhões de Transações com Cartão American Express por ano.

Comerciante de Nível 3 refere-se a um Comerciante com 10.000 a menos de 50.000 milhões de Transações com Cartão American Express por ano.

Comerciante de Nível 4 refere-se a um Comerciante com menos de 10.000 de Transações com Cartão American Express por ano.

Concessionário refere-se a um terceiro de propriedade e operação independente (incluindo um concessionário, licenciado ou capítulo), que não seja uma Afiliada licenciada por um Franqueador para operar uma franquia e que tenha celebrado um contrato por escrito com o Franqueador pelo qual apresenta consistentemente a identificação externa de forma proeminente, identificando-se com as Marcas do Franqueador ou apresentando-se ao público como membro do grupo de empresas do Franqueador.

Consumidor é definido como um titular de cartão que compra bens, serviços ou ambos.

Crédito refere-se ao montante de Cobrança reembolsado pelo Comerciante ou Fornecedor aos Clientes de Cartões por compras ou pagamentos efetuados com o Cartão.

Dados de Autenticação Sensíveis refere-se a informações relacionadas com a segurança utilizadas para autenticar os titulares de cartões e/ou autorizar transações com cartões de pagamento. Estas informações incluem, mas não se limitam a, códigos de verificação do cartão, dados completos da banda (da banda magnética ou equivalente num chip), PIN e blocos de PIN.

Dados de Conta refere-se a Dados do Titular do Cartão e/ou dados de autenticação sensíveis. Consulte Dados do Titular do Cartão e Dados de Autenticação Sensíveis.

Dados do Titular do Cartão refere-se a, pelo menos, o Número de Conta Principal (Primary Account Number, PAN) completo por si só ou o Número de Conta Principal completo mais qualquer um dos seguintes elementos: nome do titular do cartão, prazo de validade e/ou código de serviço. Consulte Dados de Autenticação Sensíveis para elementos de dados adicionais que podem ser transmitidos ou processados (mas não armazenados) como parte de uma transação de pagamento.

Dados de Transação refere-se a todas as informações exigidas pela American Express, que comprovem uma ou mais transações, incluindo informações obtidas no ponto de venda, informações obtidas ou geradas durante a Autorização e o Envio, e qualquer Estorno.

Data de Notificação refere-se à data em que a American Express fornece às entidades emissoras a notificação final de um Incidente de Dados. Esta data está dependente da receção por parte da American Express do relatório forense final ou da análise interna e será determinada a critério exclusivo da American Express.

Dispositivo com Introdução de PIN tem o significado que lhe é atribuído no presente Glossário de Termos para o Ponto de Interação (Point of Interaction, POI) da Segurança de Transação de PIN (PIN Transaction Security, PTS), Requisitos de Segurança Modular, que está disponível em www.pcisecuritystandards.org.

Dispositivo Eletrónico Compatível refere-se a um dispositivo de ponto de venda com uma aprovação/certificação EMVCo (www.emvco.com) válida e atualizada e com a capacidade de processar Transações por Cartões Eletrónicos compatíveis com AEIPS.

Documentação de Validação refere-se ao AOC produzido no seguimento de uma Avaliação de Segurança no Local Anual ou SAQ, do AOSC e os resumos das conclusões produzidas no seguimento de Verificações Trimestrais de Rede ou do Certificado do Programa de Melhoria de Tecnologias de Segurança Anual.

Encriptação Ponto a Ponto (P2PE) refere-se a uma solução que protege os dados de conta por meio de criptografia desde o ponto em que o comerciante aceita o cartão de pagamento até ao ponto de descodificação seguro.

Entidade Emissora de Cartões refere-se a qualquer Entidade (incluindo American Express e respetivas Afiliadas) licenciada pela American Express ou uma Afiliada da American Express para emitir Cartões e para se envolver no negócio de emissão de Cartões.

Especificações EMV refere-se às especificações emitidas pela EMVCo, LLC, que estão disponíveis em www.emvco.com.

Fornecedor de Serviços de Nível 1 refere-se a um Fornecedor de Serviços com 2,5 milhões de Transações com Cartão American Express ou mais por ano; ou qualquer Fornecedor de Serviços que a American Express considere de Nível 1.

Fornecedor de Serviços de Nível 2 refere-se a um Fornecedor de Serviços com menos de 2,5 milhões de Transações com Cartão American Express por ano; ou qualquer Fornecedor de Serviços não considerado de Nível 1 pela American Express.

Fornecedor de Verificação Aprovado (Approved Scanning Vendor, ASV), refere-se a uma Entidade qualificada pelo Payment Card Industry Security Standards Council, LLC com o objetivo de validar o cumprimento de determinados requisitos do PCI DSS, ao executar verificações de vulnerabilidade de ambientes que estão em contacto com a Internet.

Fornecedores de Serviços refere-se aos processadores autorizados, aos processadores de terceiros, integradores de Sistemas POS e a quaisquer outros fornecedores de Comerciantes de Sistemas POS ou a outras soluções ou serviços de processamento de pagamentos.

Franqueador refere-se ao operador de um negócio que licencia pessoas ou Entidades (Concessionários) para que estes possam efetuar a distribuição de bens e/ou serviços ou operar utilizando a Marca do operador; fornece assistência aos Concessionários durante as suas atividades ou influencia o método de funcionamento dos Concessionários; e requer o pagamento de uma taxa por parte dos Concessionários.

Incidente de Dados refere-se a um incidente que compromete ou que se suspeita que compromete as chaves de encriptação da American Express ou, pelo menos, um número de conta de Cartão American Express no qual existe:

- acesso ou utilização não autorizados das Chaves de Encriptação, Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (ou uma combinação de cada) que são armazenados, processados ou transmitidos no sistema, equipamentos e/ou redes (ou componentes dos mesmos) do Comerciante ou do Fornecedor, ou a utilização dos mesmos determinada, fornecida ou disponibilizada pelo Comerciante ou Fornecedor;
- utilização destas Chaves de Encriptação, Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (ou uma combinação de cada) não efetuada em conformidade com o Acordo; e/ou
- suspeita ou confirmação de perda, roubo ou apropriação indevida por qualquer meio, material, registo ou informação que contenha estas Chaves de Encriptação, Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (uma combinação de cada).

Informação do Cliente do Cartão refere-se às informações de Clientes de Cartões American Express e as Transações do Cartão, incluindo nomes, moradas, números de contas de cartões e número de identificação de cartões (CID).

Investigador Forense do PCI (PFI) refere-se a uma entidade que foi aprovada pelo Payment Card Industry Security Standards Council, LLC para a execução de investigações forenses quando tiver ocorrido uma falha nos dados do cartão de pagamentos ou os mesmos tiverem sido comprometidos.

Modelo do Relatório Final de Incidentes Forenses refere-se ao modelo disponível junto do Security Standards Council do PCI, que se encontra disponível em www.pcisecuritystandards.org.

Nível de Comerciante refere-se à designação que atribuímos aos Comerciantes relacionada com as respetivas obrigações de validação de conformidade com o PCI DSS, conforme descrito na Secção 2, "Programa de Conformidade do PCI DSS (Importante Validação Periódica dos seus Sistemas)".

Número de Conta Principal (Primary Account Number, PAN) tem o significado que lhe foi atribuído à data no Glossário de Termos do PCI DSS.

Número do Cartão refere-se ao número de identificação único que a Entidade Emissora atribui ao Cartão quando este é emitido.

Número de Cartão Comprometido refere-se a um número de conta de Cartão American Express relacionado com um Incidente de Dados.

Partes Abrangidas refere-se a alguns ou a todos os colaboradores, agentes, representantes, subcontratantes, Processadores, Fornecedores de Serviços, fornecedores de sistemas de equipamento de ponto de venda (POS) ou sistemas ou soluções de processamento de pagamentos, Entidades associadas à sua conta de Comerciante American Express e qualquer outra parte a quem possa disponibilizar acesso a Dados do Titular do Cartão ou Dados de Autenticação Sensíveis (ou ambos) em conformidade com o Acordo.

Payment Card Industry Data Security Standard (PCI DSS) significa Padrão de Segurança de Dados do Setor de Cartões de Pagamento e está disponível em www.pcisecuritystandards.org.

PCI DSS significa Padrão de Segurança de Dados do Setor de Cartões de Pagamento e está disponível em www.pcisecuritystandards.org.

Período do Evento de Acidente de Dados refere-se ao período de intrusão (ou um período determinado como similar) indicado no relatório forense final (por exemplo, um relatório do PFI) ou, se não for conhecido, até 365 dias antes da última Data de Notificação de Números de Cartões potencialmente comprometidos envolvidos num evento de Comprometimento de Dados que nos tenha sido comunicado.

Portal, O refere-se ao sistema de relatórios fornecido pelo administrador do Programa PCI da American Express selecionado pela American Express. Os Comerciantes e Fornecedores de Serviços são obrigados a utilizar O Portal para enviar toda a documentação de validação PCI à American Express.

Processador refere-se a um fornecedor de serviços aos Comerciantes que possibilita o processamento de autorizações e submissões à rede da American Express.

Programa, O refere-se ao Programa de Conformidade do PCI da American Express.

Programa de Análise Direcionada refere-se a um programa que fornece identificação antecipada de um possível comprometimento dos dados do Titular do Cartão no seu Ambiente de Dados do Titular do Cartão (CDE). Consulte a Secção 5, "Programa de Análise Direcionada (Targeted Analysis Programme, TAP)".

Programa de Melhoria de Tecnologias de Segurança (STEP) refere-se ao programa da American Express no qual os Comerciantes são incentivados a implementar tecnologias que melhoram a segurança de dados.

Questionário de Autoavaliação (Self-Assessment Questionnaire, SAQ), refere-se a uma ferramenta de autoavaliação criada pelo Payment Card Industry Security Standards Council, LLC, que se destina a avaliar e comprovar a conformidade com o PCI DSS.

Registo de Cobrança refere-se a um registo passível de reprodução (tanto em papel como em formato eletrónico) de uma Cobrança que cumpre os nossos requisitos e contém o Número do Cartão, a Data da Transação, o montante em dólares, a Aprovação, a assinatura do Titular do Cartão (se aplicável) e outras informações.

Registo de Crédito refere-se a um registo de Crédito que cumpre os nossos requisitos.

Requisitos de Segurança de PIN do PCI refere-se aos Requisitos de Segurança de PIN do Setor de Cartões de Pagamento e está disponível em www.pcisecuritystandards.org.

Requisitos do Payment Card Industry Security Standards Council (PCI SSC) significa o conjunto de normas e requisitos relacionados com a segurança e proteção dos dados dos cartões de pagamento, incluindo o PCI DSS e o PA DSS, disponível em www.pcisecuritystandards.org.

Solução Aprovada de Encriptação Ponto a Ponto (P2PE), incluída na lista de soluções validadas do PCI SSC ou validadas por um Assessor de Segurança Qualificado do PCI SSC de uma Empresa P2PE.

Sistema de Ponto de Venda (POS) refere-se a um sistema ou equipamento de processamento de informações, constituído por um terminal, computador pessoal, caixa registadora eletrónica, leitor "contactless" ou motor ou processo de pagamento, utilizado por um Comerciante para obter autorizações ou recolher dados de transação, ou ambos.

Tecnologia de Mitigação de Riscos significa soluções tecnológicas que melhoram a segurança dos Dados dos Titulares de Cartões American Express e dos Dados de Autenticação Sensíveis conforme determinado pela American Express. Para ser considerada Tecnologia de Mitigação de Riscos, o Comerciante ou Fornecedor tem de demonstrar a utilização efetiva da tecnologia de acordo com a sua conceção e finalidade pretendida. Os exemplos incluem, entre outros: EMV, Encriptação Ponto a Ponto e utilização de tokens.

Titular do Cartão refere-se a um cliente ao qual é emitido um cartão de pagamento ou a qualquer pessoa autorizada a utilizar o cartão de pagamento.

Token refere-se ao token criptográfico que substitui o PAN, com base num determinado índice para um valor imprevisível.

Transação EMV refere-se a uma Transação com um cartão de circuitos integrados (por vezes denominado "Cartão CI", "cartão eletrónico", "cartão inteligente", "cartão EMV" ou "ICC") efetuada num terminal de um ponto de venda compatível com cartão CI, que possui um tipo de aprovação EMV válida e atual. Os tipos de aprovação EMV estão disponíveis em www.emvco.com.

Transação refere-se a uma Cobrança, Crédito, Adiantamento de Numerário (ou outro acesso a numerário) ou Transação por ATM concluída através de um Cartão.

Transações de Pagamentos Iniciados pelo Comprador (Buyer Initiated Payment, BIP), refere-se a uma solução de pagamento digital que permite aos compradores programar rápida e eficientemente pagamentos aos fornecedores (associado a cartões empresariais).

Secção 9 Sites Úteis

Segurança de Dados da American Express: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com