



Security
Standards Council®

Padrão: Padrão de Segurança de Dados do PCI (PCI DSS)

Data: março de 2016

Autor: Grupo de interesse especial em garantia de segurança de terceiros e responsabilidades compartilhadas
PCI Security Standards Council

Suplemento de informações:

Garantia de segurança de terceiros

Alterações no documento

Data	Versão do documento	Descrição	Páginas
Agosto de 2014	1.0	Primeira versão	Todas
Março de 2016	1.1	Conteúdo expandido e revisado com base no Grupo de interesse especial em responsabilidades compartilhadas	Vários

Índice

Alterações no documento	i
1 Introdução	1
1.1 Uso pretendido	2
1.2 Terminologia.....	2
1.3 Público.....	2
2 Exemplos de prestadores de serviços terceirizados.....	4
3 Due diligence do prestador de serviços terceirizado	5
3.1 Determinação do escopo dos serviços fornecidos	6
3.2 Pesquisa de due diligence do prestador de serviços terceirizado	6
3.2.1 Adquirente/bandeiras de cartão de pagamento	9
3.2.2 Documentação de validação do prestador de serviços terceirizado	9
3.2.3 Listas e sites de provedores validados de bandeiras de cartões de pagamento	12
3.3 Realização da avaliação de risco.....	13
3.4 Documentação dos resultados.....	15
4 Contratação do prestador de serviços terceirizado	16
4.1 Acordo de confidencialidade (Non-Disclosure Agreement, NDA)	16
4.2 Estabelecer expectativas	16
4.3 Obter transparência	17
4.4 Estabelecer comunicações	17
4.5 Solicitar evidência	18
4.6 Obter informações sobre a conformidade do PCI DSS	18
4.7 Frequência da revisão.....	18
4.8 Mapeamento de serviços de terceiros para os requisitos aplicáveis do PCI DSS	19
5 Acordos por escrito, políticas e procedimentos	20
5.1 Acordos entre prestadores de serviços terceirizados em conformidade com o PCI DSS em comparação a prestadores de serviços terceirizados sem conformidade com o PCI DSS	20
5.2 Considerações ao estabelecer acordos, políticas e procedimentos.....	21
5.3 Considerações adicionais	23
5.3.1 Matriz de responsabilidades	23
5.3.2 Violações de dados	24
5.3.3 Considerações pós-rescisão sobre TPSPs e seus clientes	24
5.3.4 Terceirização da funcionalidade fornecida (TPSPs integrados)	25
5.3.5 Perda do status de conformidade.....	26
6 Manutenção de relacionamentos e monitoramento de prestadores de serviços terceirizados	27
6.1 Desenvolvimento de um programa de monitoramento de prestadores de serviços terceirizados	27
6.1.1 Definição do escopo do ambiente de dados do titular do cartão (Cardholder Data Environment, CDE).....	28
6.1.2 Manutenção de um inventário de prestadores serviços terceirizados	28

6.1.3	Procedimento para monitoramento de prestador de serviços terceirizado.....	28
6.2	Outras considerações	30
6.2.1	O prestador de serviços terceirizado não fornece as informações solicitadas	30
6.2.2	O prestador de serviços terceirizado não validou a conformidade do PCI DSS.....	30
6.2.3	O prestador de serviços de terceiros valida a conformidade do PCI DSS através da inclusão na avaliação do PCI DSS da entidade	31
6.2.4	O serviço ou processo existente ou novo não é compatível com PCI DSS ou fará com que a entidade ou TPSP não estejam em conformidade com o PCI DSS	32
Anexo A:	Pontos de discussão de alto nível para determinar a responsabilidade	34
Anexo B:	Exemplo da matriz de responsabilidades do PCI DSS	43
Agradecimento		45
Sobre o PCI Security Standards Council		48

1 Introdução

À medida que as entidades trabalham visando ao objetivo de alcançar e manter a conformidade contínua com o PCI DSS, elas podem optar por utilizar prestadores de serviços terceirizados (third-party service providers, TPSPs) para atingir seus objetivos. As entidades podem usar um TPSP para armazenar, processar ou transmitir dados do titular do cartão em nome da entidade ou gerenciar componentes do ambiente de dados do titular do cartão (cardholder data environment, CDE) da entidade, como roteadores, firewalls, bancos de dados, segurança física e/ou servidores. Esses TPSPs podem se tornar parte integrante do ambiente de dados do titular do cartão da entidade e impactar a conformidade do PCI DSS de uma entidade, bem como a segurança do ambiente de dados do titular do cartão.

No entanto, o uso de um TPSP não isenta a entidade da responsabilidade final por sua própria conformidade com o PCI DSS nem a isenta da responsabilidade e obrigação de garantir que seus dados do titular do cartão (cardholder data, CHD) e seu CDE estejam seguros. Políticas e procedimentos claros devem, portanto, ser estabelecidos entre a entidade e seu(s) TPSP(s) para todos os requisitos de segurança aplicáveis, e medidas adequadas devem ser desenvolvidas para gerenciar e relatar em relação aos requisitos.

Um programa de garantia de terceiros robusto e devidamente implementado auxilia uma entidade a assegurar que os dados e sistemas que ela atribui aos TPSPs sejam mantidos de forma segura e em conformidade. A due diligence e a análise de risco adequadas são componentes críticos na seleção de qualquer TPSP.

Esta orientação foca principalmente no seguinte:

Due diligence do prestador de serviços terceirizado: A análise minuciosa dos candidatos através de due diligence cuidadosa, antes de estabelecer um relacionamento, auxilia as entidades na revisão e seleção de TPSPs com habilidades e experiência apropriadas para a contratação.

Correlação de serviço com os requisitos do PCI DSS: Compreender como os serviços prestados pelos TPSPs correspondem aos requisitos aplicáveis do PCI DSS ajuda a entidade a determinar o possível impacto à segurança de utilizar TPSPs no ambiente de dados do titular do cartão da entidade. Essas informações também podem ser usadas para determinar e entender quais requisitos do PCI DSS serão aplicados e satisfeitos pelo TPSP, e quais serão aplicados e atendidos pela entidade.

Observação: a responsabilidade final pela conformidade é da entidade, independentemente de como as responsabilidades específicas possam ser alocadas entre uma entidade e seu(s) TPSP(s).

Acordos por escrito e políticas e procedimentos: Acordos por escrito detalhados promovem a consistência e a compreensão mútua entre a empresa e seu(s) TPSP(s) em relação às suas respectivas responsabilidades e obrigações com relação aos requisitos de conformidade do PCI DSS.

Monitorar o status de conformidade do prestador de serviços terceirizados: Conhecer o status de conformidade do PCI DSS do TPSP ajuda a fornecer à empresa contratando um TPSP garantia e conscientização quanto ao fato de o TPSP estar em conformidade com os requisitos aplicáveis para os serviços prestados. Se o TPSP oferecer uma variedade de serviços, esse conhecimento ajudará a entidade a determinar quais serviços do TPSP estarão dentro do escopo da avaliação do PCI DSS da entidade.

1.1 Uso pretendido

O objetivo do presente suplemento de informações é fornecer orientação para entidades contratando TPSPs com quem os CHD são compartilhados ou que podem afetar a segurança dos CHD, conforme exigido pelo Requisito 12.8 do PCI DSS¹. Esta orientação adicional para o Requisito 12.8 do PCI DSS¹ destina-se a auxiliar as entidades e os TPSPs a entender melhor suas respectivas funções ao atender a este requisito.

As informações contidas neste documento destinam-se à orientação suplementar e não substituem, anulam ou estendem os requisitos do PCI DSS. Em última análise, a entidade é responsável por garantir sua própria conformidade com o PCI DSS, esteja um TPSP envolvido ou não. Como as responsabilidades são alocadas entre uma entidade e seu(s) TPSP(s), muitas vezes depende do relacionamento e dos serviços específicos que estão sendo fornecidos. Esta orientação não substitui a avaliação de risco adequada e a conformidade com a orientação não assegura a conformidade com o Requisito 12.8¹, etc.

1.2 Terminologia

Os seguintes termos são usados ao longo deste documento:

- **Entidade** – Uma entidade é qualquer organização que tem a responsabilidade de proteger os dados do cartão e pode utilizar um prestador de serviços terceirizado para apoiá-la em atividades de processamento de cartões ou para proteger dados de cartões.
- **TPSP (Third-party Service Provider, Prestador de serviços terceirizado)** – Conforme definido no *Glossário de termos, abreviações e acrônimos do PCI DSS e PA-DSS*, um prestador de serviços é uma entidade de negócios que não é uma bandeira de pagamento, diretamente envolvida no processamento, armazenamento ou transmissão de dados do titular do cartão em nome de outra entidade. Isso inclui também as empresas que prestam serviços que controlam ou podem afetar a segurança dos dados do titular de cartão. Há muitos tipos de negócios que podem se encaixar na categoria de “prestador de serviços”, dependendo dos serviços prestados. Mais comumente, um TPSP pode ser uma entidade legalmente separada; mas também pode ser uma unidade de negócios separada ou um componente da entidade sob avaliação — por exemplo, um prestador de serviços interno — onde o prestador está fora do controle de gestão direta da entidade avaliada.
- **TPSP integrado ou em cadeia** – Um TPSP integrado ou em cadeia é qualquer entidade contratada por seus serviços por outro prestador de serviços terceirizado para fins de prestação de serviços.

1.3 Público

Entidades envolvendo um prestador de serviços terceirizado (por exemplo, emissores, comerciantes, adquirentes ou outros prestadores de serviços) – Entidades que envolvam TPSPs para armazenamento, transmissão, processamento de dados do titular do cartão ou fornecimento de serviços que controlam ou possam afetar a segurança dos dados do titular do cartão podem se beneficiar dessas diretrizes. As recomendações fornecidas neste documento destinam-se a auxiliar as entidades no desenvolvimento de um maior entendimento sobre a utilização de TPSPs e o impacto subsequente ao ambiente de dados do titular do cartão da entidade, o impacto nas responsabilidades de conformidade do PCI DSS da entidade, bem como fornecer orientação sobre como atender ao objetivo do Requisito 12.8¹ do PCI DSS que regula os TPSPs.

¹ Esta referência é ao PCI DSS v3.1 – Abril de 2015

Prestadores de serviços terceirizados – Este documento de orientação também pode fornecer informações úteis para que os TPSPs entendam suas responsabilidades frente às entidades para as quais estão fornecendo serviços. Além disso, um TPSP pode depender da conformidade de um TPSP integrado ou em cadeia para atender a conformidade geral de um serviço. O TPSP deve entender a melhor forma de se envolver com seu(s) parceiro(s) para garantir a conformidade do PCI DSS quanto aos serviços oferecidos. O Requisito 12.9² do PCI DSS também exige que os prestadores de serviços confirmem suas responsabilidades de proteger os dados do titular do cartão dos clientes ou o ambiente de dados do titular do cartão dos clientes, por escrito, aos clientes do TPSP.

Adquirentes (também chamados “bancos adquirentes”, “bancos comerciais” ou “instituições financeiras adquirentes”) – Como uma entidade que inicia e mantém relacionamentos com comerciantes para a aceitação de cartões de pagamento, um adquirente é responsável por garantir que os comerciantes em seu portfólio estejam usando TPSPs seguros.

² Esta referência é ao PCI DSS v3.1 – Abril de 2015

2 Exemplos de prestadores de serviços terceirizados

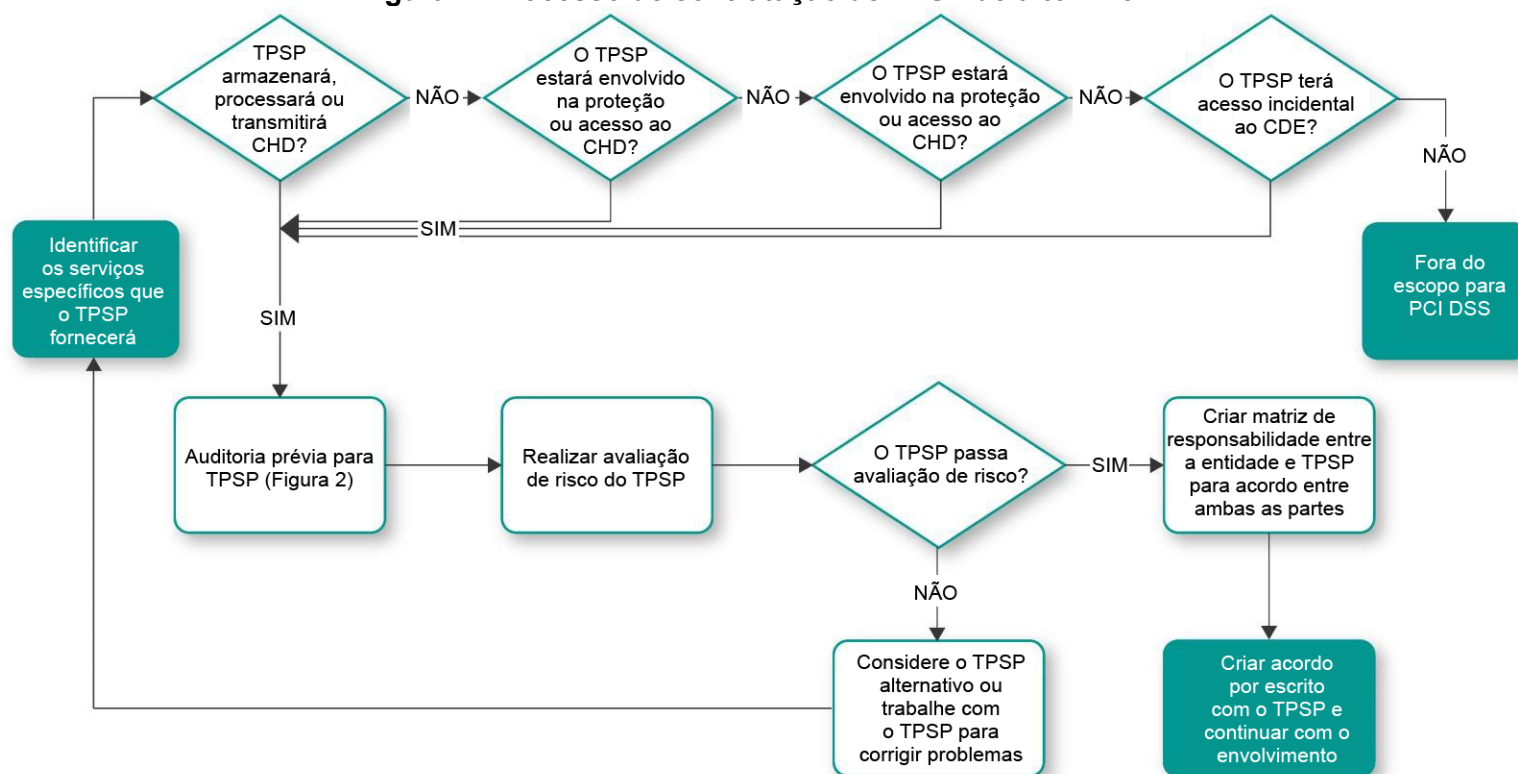
Abaixo há exemplos de tipos de serviços e prestadores com os quais uma entidade pode trabalhar:

- Empresas envolvidas no armazenamento, processamento e/ou transmissão de dados do titular do cartão (CHD). Os prestadores de serviços terceirizados nesta categoria podem incluir:
 - Entidades que prestam atendimento ao cliente e call center
 - Provedores de pagamento de e-commerce
 - Empresas que processam pagamentos em nome da entidade, como um parceiro ou revendedor
 - Serviços de verificação de fraudes, serviços de relatórios de crédito, agências de cobrança
 - Processadores de terceiros
 - Entidades que oferecem serviços de gateway de processamento
 - Cobradores de dívidas de terceiros/processos de cobrança
- Empresas envolvidas na proteção dos dados do titular do cartão. Os TPSPs nesta categoria podem incluir:
 - Empresas que fornecem destruição segura de mídia eletrônica e física
 - Instalações de armazenamento seguro para mídia eletrônica e física
 - Empresas que transformam dados do titular do cartão com tokenização ou criptografia
 - Terceiros de e-commerce ou de aplicativos móveis que fornecem software como serviço
 - Provedores de gerenciamento de chaves, como serviços key-injection ou organizações de suporte de criptografia (encryption-support organizations, ESO)
- Empresas de ponto de venda (ou integradores/revendedores) envolvidas na instalação, manutenção, monitoramento ou suporte de qualquer outra forma de seus sistemas.
- Organizações envolvidas na proteção do ambiente de dados do titular do cartão (CDE). Os TPSPs nesta categoria podem incluir:
 - Prestadores de serviços de infraestrutura
 - Provedores gerenciados de firewall/roteador
 - Provedores de hospedagem seguros de data-center
 - Serviços de monitoramento para alertas críticos de segurança, como sistemas de detecção de invasão (intrusion-detection systems, IDS), antivírus, detecção de alterações, monitoramento de conformidade, monitoramento de registro de auditoria, etc.
- Organizações que podem ter acesso incidental aos CHD ou ao CDE. Acesso incidental é o acesso que pode acontecer como consequência da atividade ou do trabalho. Os TPSPs nesta categoria podem incluir:
 - Prestadores de serviços e canais de entrega de TI gerenciados
 - Empresas que fornecem desenvolvimento de software, como aplicativos da Web
 - Prestadores de serviços de manutenção — por exemplo, serviços de climatização (AVAC) ou limpeza

3 Due diligence do prestador de serviços terceirizado

Firmar parceria com os TPSPs corretos é uma tarefa desafiadora. As considerações iniciais devem incluir medidas para proteger dados do titular do cartão, dados financeiros e outros dados confidenciais e pessoais, e cumprir as leis e regulamentos locais. Cada empresa deve desenvolver suas próprias políticas e procedimentos, bem como seus próprios critérios para pré-seleção e gerenciamento de possíveis TPSPs durante o processo de análise. Deve-se enviar todos os esforços para exercer a quantidade apropriada de due diligence e realizar uma avaliação de risco dos TPSPs pré-selecionados. Abaixo vemos um exemplo de um fluxo de processo de alto nível que uma entidade pode incluir como parte de sua due diligence ao contratar TPSPs. Observe que este processo não é exaustivo. Isso significa uma diretriz para ajudar as empresas a criar um programa apropriado de due diligence para contratar TPSPs.

Figura 1: Processo de contratação de TPSP de alto nível



3.1 Determinação do escopo dos serviços fornecidos

Ao contratar um TPSP, inicialmente a entidade deve considerar determinar o escopo do envolvimento do TPSP com relação ao armazenamento, processamento ou transmissão dos dados do titular do cartão, e o efeito resultante sobre a segurança do CDE. Como o envolvimento e os serviços do TPSP podem afetar o nível de risco assumido pela entidade ao processar transações de pagamento, a due diligence minuciosa é fundamental para determinar qual TPSP é apropriado e quais serviços de terceiros podem ser necessários.

Definir o nível de envolvimento de um TPSP é crucial para compreender o risco geral assumido pela entidade relacionada à conformidade com o PCI DSS. A entidade pode optar por contratar um parceiro externo para auxiliar na avaliação do escopo dos serviços a serem prestados pelo TPSP e a aplicabilidade desses serviços à conformidade do PCI DSS da entidade. Perguntas que podem ajudar neste processo incluem:

- Considerando o ecossistema de pagamento atual e os canais de pagamento, quais serviços (segurança, acesso, etc.) afetariam ou impactariam o CDE e/ou os CHD? Como os serviços são estruturados nas instalações do TPSP?
- Que tecnologia e componentes do sistema são usados pelo TPSP para os serviços prestados?
- Terceiros adicionais são usados pelo TPSP na entrega do serviço fornecido?
- Que outros processos/serviços centrais estão alojados nas instalações do TPSP que podem afetar os serviços prestados? Que tecnologia é usada para esses processos/serviços centrais?
- Quantas instalações o TPSP possui em que os CHD estão ou estarão localizados?

Observação: o escopo e os serviços a serem fornecidos por um TPSP dependerão dos fatos e circunstâncias específicos, e dos serviços fornecidos. Embora a lista de perguntas acima possa ser útil para determinar o escopo e os serviços, ela não é exaustiva. Cada empresa que busca contratar um TPSP deve determinar o que é relevante à luz das circunstâncias, do ambiente de pagamento da organização, a função proposta do TPSP e outros fatores determinados como importantes através da due diligence minuciosa.

3.2 Pesquisa de due diligence do prestador de serviços terceirizado

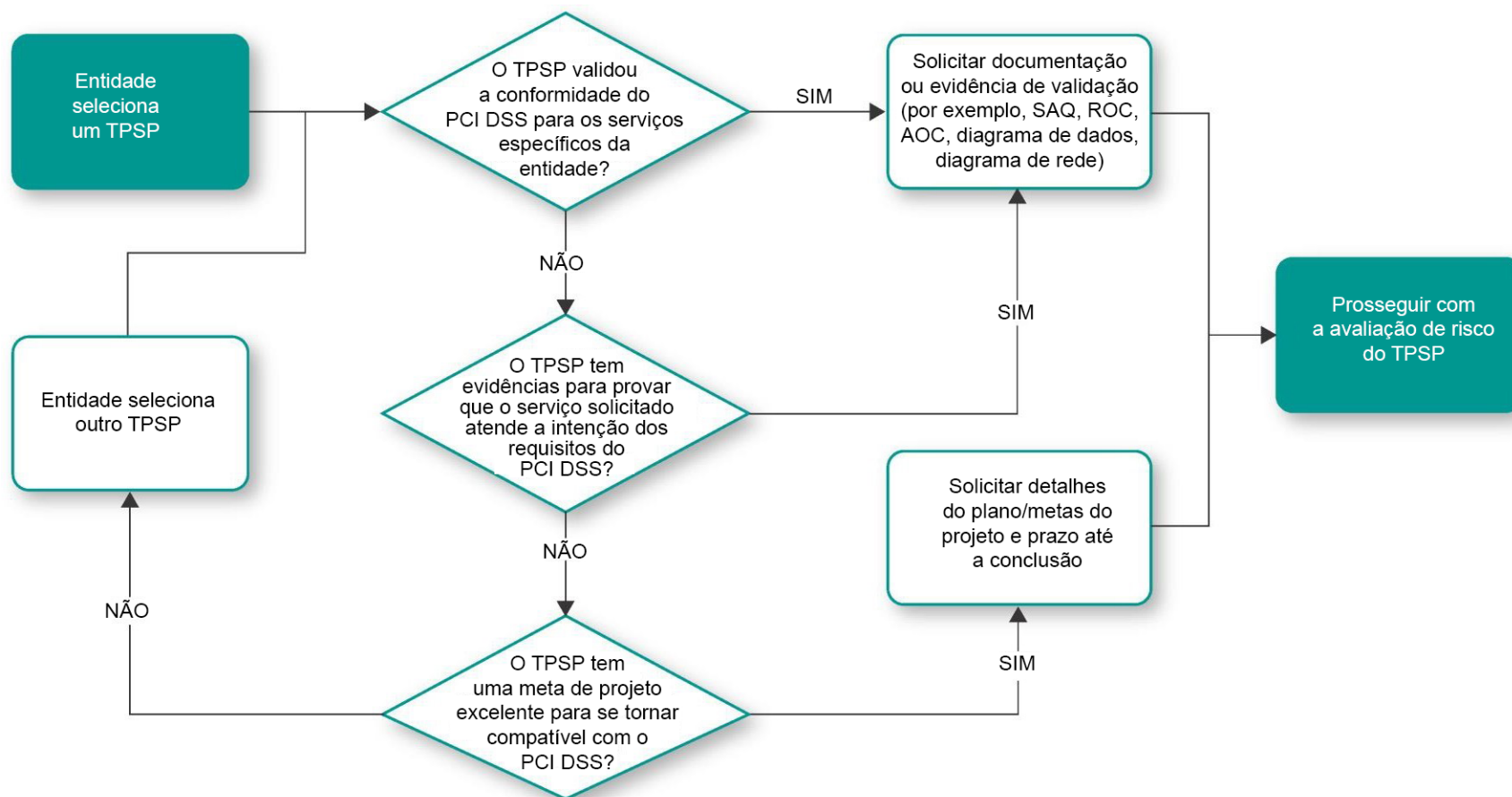
Com base nos serviços fornecidos pelo TPSP, a entidade precisará determinar um caminho de diligência devida para identificar o impacto que um TPSP tem dentro do escopo do PCI DSS da entidade. A entidade deve considerar começar com uma análise preliminar do TPSP para garantir que a contratação não tenha impacto negativo na conformidade com o PCI DSS da entidade. Essa pesquisa pode incluir precauções como consultoria com o adquirente, revisão das listagens e sites de prestadores de serviços de bandeira de cartões de pagamento participantes e solicitação de documentação de validação do PCI DSS. Observe que nem todas as bandeiras de cartão de pagamento têm listagens de prestadores de serviços. No entanto, algumas regras de bandeira de cartão de pagamento exigem que certos tipos de prestadores de serviços sejam registrados com a respectiva bandeira do cartão. Considerações de risco adicionais (que podem estar fora do escopo dos requisitos do PCI DSS) incluem avaliar os TPSPs:

- Estabilidade financeira antes da assinatura ou renovação do contrato
 - Reputação, incluindo a análise de reclamações e litígios relatados
- Experiência no fornecimento ou na implementação dos serviços propostos, incluindo a capacidade do TPSP de manter o serviço ao longo do tempo e experiência de gerenciamento

- Cobertura do seguro
- Uso de TPSPs integrados para fornecer os serviços solicitados e avaliação da capacidade do TPSP integrado para executar esses serviços
- Conformidade com as políticas de segurança de terceiros da sua empresa
- Violações, se ocorreram, e o status de resolução de cada violação
- Prontidão para continuidade dos negócios
- Consideração de qualquer possível risco legal

O fluxograma de trabalho na Figura 2, abaixo, detalha um fluxo de alto nível potencial para uma empresa seguir ao realizar uma pesquisa de due diligence sobre potenciais TPSPs. Como observado acima, no entanto, cada empresa deve determinar o processo apropriado de due diligence em vista de seu próprio CDE. Parte da due diligence incluirá uma decisão sobre qual forma de evidência será aceitável, inicialmente e durante todo o período do relacionamento, quanto à conformidade do TPSP com o PCI DSS.

Figura 2: Exemplo de processo de due diligence



As entidades podem precisar consultar seu adquirente ou marca de cartão de pagamento para determinar se há requisitos para envolver um TPSP. Consulte a Seção 3.2.1 para obter mais informações.

3.2.1 **Adquirente/bandeiras de cartão de pagamento**

Como parte do processo de due diligence e antes de continuar com a pesquisa, uma entidade também pode querer consultar seu adquirente ou bandeira de cartão de pagamento³ para garantir que os serviços do TPSP sejam aprovados para uso pelo adquirente ou pela bandeira de cartão de pagamento e que não haja restrições com relação aos TPSPs. Em alguns casos, um adquirente ou bandeira de cartão de pagamento pode não permitir a contratação de TPSPs devido a um risco que já tenha sido identificado anteriormente

3.2.2 **Documentação de validação do prestador de serviços terceirizado**

A entidade também pode considerar solicitar a documentação de validação do TPSP que demonstra que este está em conformidade com o PCI DSS. A maneira como e se um TPSP deve validar a conformidade do PCI DSS é definida pelas bandeiras de cartão de pagamento e a documentação de validação necessária pode variar. Isso, por sua vez, afeta os tipos de documentação de conformidade que uma entidade pode esperar receber do TPSP. Consulte os sites das bandeiras de cartões de pagamento para obter mais informações sobre programas específicos de conformidade da bandeira ou entre em contato diretamente com as bandeiras de cartão de pagamento.

O nível de documentação deve ser proporcional ao nível de risco e ao impacto que o TPSP apresenta à conformidade do PCI DSS da entidade. A documentação deve ser suficiente para confirmar que os serviços fornecidos são cobertos pela avaliação do PCI DSS do TPSP e para identificar que os requisitos do PCI DSS que foram avaliados tenham sido cumpridos. A documentação também deve incluir informações relacionadas a quaisquer serviços fornecidos pelo TPSP em outros países.

Consequentemente, uma entidade da qual é exigida a validação de sua conformidade através de uma avaliação completa no local pode contar com a validação autoavaliada de seu TPSP, se este for classificado para realizar a autoavaliação e se isso estiver alinhado com a posição de gerenciamento de risco da empresa e os programas de conformidade de bandeira de pagamento aplicáveis.

Como parte do processo de due diligence, a seguinte documentação pode ser obtida de TPSPs que foram validados como estando em conformidade com PCI DSS, conforme aplicável. A lista também contém recomendações para analisar a documentação de validação que pode ser fornecida à entidade. A documentação de validação fornecida à entidade deve abranger o(s) serviço(s) sendo entregue(s) pelo TPSP para a entidade para ajudar a garantir que os serviços fornecidos sejam cobertos pela validação de conformidade do TPSP:

- **Relatório de conformidade (Report on Compliance, ROC):** Preenchido por um avaliador de segurança interno (Internal Security Assessor, ISA) ou por um assessor de segurança qualificado externo (Qualified Security Assessor, QSA). Seções relevantes do ROC podem ser suficientes para demonstrar o escopo de uma avaliação do PCI DSS e o status de conformidade. Isso pode ser desnecessário se o AOC cobrir os serviços necessários.
 - Se forem usados controles de compensação, determine por que o requisito original não pode ser atendido; entenda qual é o controle, como está atendendo o objetivo e rigor do requisito original, e como o controle está sendo mantido.

Observação: *é possível que um TPSP possa optar por não compartilhar determinados aspectos ou qualquer parte do seu ROC se informações confidenciais forem incluídas ou quando a liberação do documento puder comprometer a confidencialidade. Informações alternativas podem incluir um*

³ Informações de contato da bandeira de cartão de pagamento podem ser encontradas no site do PCI SSC:
https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands

onde informações confidenciais podem ser analisadas, quando necessário, ou uma reunião presencial para permitir a visualização da documentação. Além disso, muitos QSAs fornecem uma carta em papel timbrado da empresa, que pode ser usada se o TPSP não quiser compartilhar informações potencialmente confidenciais

- **Atestado de conformidade (Attestation of Compliance, AOC):** Um “Atestado de conformidade para avaliações no local” totalmente assinado – Prestadores de serviços⁴ pode ser fornecido à entidade mediante solicitação. O modelo e as informações para preencher o documento podem ser encontrados no site do PCI SSC.
 - Examine o nome e o tipo de serviços avaliados na Seção 2A, “Verificação do escopo”, para validar os serviços fornecidos pelo TPSP. Exemplos são “Provedor de hospedagem” e “Processamento de pagamento”.
 - Analise os relacionamentos com outros TPSPs para entender se existem serviços adicionais que podem precisar de avaliação ou inclusão.
 - Analise o AOC para determinar se o TPSP tem requisitos que não estão em conformidade e que devem ser cobertos pelos serviços prestados.
 - É garantida a análise cuidadosa da Parte 2G, “Resumo dos requisitos testados”, pois esta contém os requisitos do PCI DSS que o TPSP testou completamente, parcialmente ou não testou para cada serviço fornecido. Para qualquer resposta “Parcial” ou “Nenhuma”, a entidade deve realizar a análise para garantir que os serviços fornecidos sejam cobertos. Se o serviço fornecido não foi coberto por esta avaliação, a entidade pode querer incluir isso em sua avaliação do PCI DSS. Observe que o PCI DSS exige que a entidade avaliada mantenha informações sobre quais requisitos do PCI DSS são administrados por cada prestador de serviços e quais são administrados pela entidade (Requisito 12.8.5⁴). Esteja ciente, no entanto, de que o PCI DSS não exige que o TPSP leve em conta todos os requisitos do PCI DSS (por exemplo, usando uma matriz de conformidade para todos os seus clientes).
- **Questionário de autoavaliação (Self-Assessment Questionnaire, SAQ) D e Atestado de conformidade para prestadores de serviços (AOC):** Preenchido pelo TPSP se estiver concluindo uma autoavaliação. Esses documentos podem ser encontrados no site do PCI SSC.
 - É garantida a análise cuidadosa da Parte 2G, “Resumo dos requisitos testados”,⁴ pois esta contém os requisitos do PCI DSS que o TPSP testou completamente, parcialmente ou não testou para cada serviço fornecido. Para qualquer resposta “Parcial” ou “Nenhuma”, a entidade deve realizar a análise para garantir que os serviços fornecidos sejam cobertos. Se o serviço fornecido não foi coberto por esta avaliação, a entidade pode querer incluir isso em sua avaliação do PCI DSS.
 - Se forem usados controles de compensação, determine por que o requisito original não pode ser atendido; entenda qual é o controle, como está atendendo o objetivo e rigor do requisito original, e como o controle está sendo mantido.
 - O Anexo D do SAQ, se fornecido, pode ser analisado a fim de entender quais requisitos são marcados como não aplicáveis ou não testados para saber se eles são aceitáveis e se estão claramente explicados.

⁴ Refere-se à versão 3.1 – Abril de 2015

- Se fornecidas, revise a Parte 2E, “Descrição do ambiente”⁵, e a Parte 2D, “Aplicativo de pagamento”⁵, para determinar se eles estão incluídos na avaliação dos serviços prestados.
- Revise a Seção 3, “Detalhes da validação e do atestado”⁵, para confirmar os resultados da avaliação.
- **Atestado do relatório de verificação ASV para conformidade de verificações (Attestation of Scan Compliance, AOSC):** Fornecido pelo provedor de verificações aprovado do TPSP se este fornecer serviços que são entregues por meio de sistemas exigidos para atender ao Requisito 11.2.2 do PCI DSS⁶. Informações sobre o AOSC são fornecidas dentro do *Guia do programa ASV do PCI DSS*, disponível no site do PCI SSC. Assim como no ROC, o AOSC pode ser redigido para remover informações confidenciais ou sigilosas.
 - O AOSC pode ser revisado quanto ao status de conformidade, data de validade da verificação e número de vulnerabilidades de falhas identificadas para determinar se os serviços específicos estão cobertos e que passaram por essas verificações.

Toda a documentação anterior também pode ter as datas de validação rastreadas com atualizações periódicas do TPSP. A entidade também deve garantir que todos os problemas anteriores de não conformidade com o TPSP tenham sido resolvidos, se o cronograma de resolução tiver sido aprovado.

Uma vez que esses diversos documentos são solicitados dos TPSPs em conformidade, a entidade também deve considerar solicitar a verificação, por escrito, de que os serviços prestados à empresa se enquadram dentro do escopo dos serviços cobertos pelo AOC, ROC, SAQ e AOSC. Isso fornece uma medida adicional de garantia de que a avaliação do PCI DSS do TPSP está alinhada com os serviços acordados. O desenvolvimento de listas de verificação de validação pode garantir que os principais campos do AOC, SAQ, ROC ou AOSC sejam analisados pela equipe de gestão.

Se o TPSP não tiver cumprido com a conformidade do PCI DSS devido a uma lacuna em aberto em seu ambiente, é responsabilidade da entidade determinar se ela aceita ou não o risco de contratar o TPSP. Recomenda-se que a entidade primeiro entenda qual lacuna o TPSP deve abordar para estabelecer a conformidade e o impacto dessa lacuna em seu próprio ambiente. Se for determinado que há um impacto, a entidade deve estabelecer um plano claro e eficaz para solucionar os problemas. Entre outras coisas, isso pode incluir a solicitação de cronogramas de projeto e marcos de metas do TPSP para determinar se a conformidade pode ser alcançada para os serviços oferecidos, dentro de um prazo aceitável para a entidade. Uma vez que o escopo e a lacuna tenham sido identificados, uma entidade pode precisar consultar seu adquirente para garantir que não haja conflito com a contratação.

Observação: *algumas bandeiras de cartão de pagamento exigem que certos tipos de prestadores de serviços façam a validação de conformidade do PCI DSS. De acordo com as regras de bandeira de cartão de pagamento, somente os prestadores de serviços listados e considerados compatíveis com o PCI DSS podem ser usados para determinados tipos de serviços.*

Se o TPSP não pretender validar a conformidade do PCI DSS ou não for necessário validar a conformidade do PCI DSS, e a entidade ainda optar por contratar o TPSP, esta será obrigada a cobrir os sistemas e processos aplicáveis do TPSP sob sua própria avaliação de conformidade do PCI DSS. Abaixo há exemplos de documentação que o TPSP pode fornecer durante uma avaliação do PCI DSS, sempre que ocorrerem alterações significativas e/ou anualmente, conforme aplicável:

⁵Refere-se ao SAQ D versão 1.1 – Julho de 2015

⁶Esta referência é ao PCI DSS v3.1 – Abril de 2015

- Um diagrama de dados de alto nível mostrando como os serviços do TPSP são compatíveis com o ambiente da entidade
- Diagramas de rede
- Evidência de metodologia de correção do sistema e, se aplicável, metodologia de codificação segura
- Lista dos TPSPs da entidade e como cada TPSP está conectado ao ambiente da entidade, juntamente com a função que estes desempenham — especificamente, quaisquer relacionamentos integrados/em cadeia
- Resultados das verificações de vulnerabilidade interna e externa do TPSP, se disponíveis
- Políticas de segurança e procedimentos operacionais

Se o TPSP ainda não estiver em conformidade, ele pode fornecer seu próprio plano de projeto para o plano de projeto da trajetória de conformidade do PCI DSS ou uma cópia de sua abordagem priorizada para o(s) serviço(s) fornecido(s), se disponível. A abordagem priorizada é uma ferramenta produzida pelo PCI SSC para ajudar as entidades a implementar os requisitos do PCI DSS em uma ordem priorizada, que aborda efetivamente os respectivos riscos. A ferramenta pode ser baixada da Biblioteca de documentos do PCI SSC em https://www.pcisecuritystandards.org/security_standards/documents.php.

Outro cenário a ser considerado é se uma entidade contrata um terceiro para aumentar sua tecnologia da informação ou sua equipe operacional, usando apenas os processos e a tecnologia da própria entidade. Nesse caso, a empresa terceirizada para incremento de pessoal provavelmente não será avaliada de forma independente por sua conformidade com o PCI DSS. No entanto, os funcionários de terceiros incorporados dentro dos processos de escopo da entidade podem precisar fazer parte do exercício de validação de conformidade da própria entidade. Isso pode incluir a demonstração de que eles seguem os próprios procedimentos da entidade, que têm seu trabalho analisado pela administração da entidade e que estão sujeitos aos mesmos controles de segurança que o restante da equipe da entidade, como, entre outros, verificações de antecedentes, treinamento de conscientização de segurança e de codificação segura.

A entidade também pode considerar o risco associado à contratação de um TPSP e como limitar a exposição ao seu escopo do PCI DSS. Além disso, a entidade pode querer considerar o esforço adicional associado à validação e à potencial resolução dos componentes e processos do sistema aplicáveis que se encaixam dentro do escopo. Por exemplo, a entidade pode considerar seu risco e impacto temporal para realizar uma avaliação interna dos sistemas e processos do TPSP em relação à contratação de um recurso externo para auditar o sistema do TPSP em nome da entidade. Por fim, como o TPSP não validou sua conformidade, os serviços fornecidos podem estar dentro do escopo da avaliação do PCI DSS da entidade e, posteriormente, podem resultar em um atraso para a validação de conformidade da entidade.

3.2.3 Listas e sites de provedores validados de bandeiras de cartões de pagamento

As bandeiras de cartões de pagamento podem manter listas dos TPSPs validados que satisfaçam programas de inscrição de bandeiras específicas, que normalmente incluem requisitos para atingir e manter a conformidade do PCI DSS. É importante que uma entidade compreenda o escopo da validação e os serviços listados. Observe que a ausência de um TPSP de uma lista não impede a contratação do prestador de serviços, uma vez que alguns TPSPs optam por não serem listados, embora tenham atingido a conformidade com o PCI DSS. Da mesma forma, a inclusão de um prestador de serviços em uma lista publicada não garante que os serviços aplicáveis à contratação da entidade estão incluídos

na validação de conformidade ou que todos os requisitos do PCI DSS, que uma entidade deseja que o TPSP gerencie em seu nome, estão incluídos no serviço validado. Dependendo dos serviços fornecidos pelo TPSP à entidade, as informações encontradas nas listagens dos prestadores de serviços de bandeiras de cartões de pagamento podem não fornecer a garantia necessária. Podem ser necessárias informações adicionais do TPSP para os serviços prestados.

3.3 Realização da avaliação de risco

Recomenda-se que uma entidade realize uma avaliação de risco completa em seu TPSP, com base em uma metodologia aceita pela indústria. Compreender o nível de risco associado à contratação de um TPSP ajudará a entidade em seu processo de tomada de decisão. Uma entidade pode precisar criar um programa de due diligence escalonado com árvores de decisão para lidar com diferentes níveis de risco, dependendo de vários fatores como:

- A magnitude e o tipo dos serviços fornecidos pelo TPSP (por exemplo, um único prestador de serviços, provedor de nuvem, etc.)
- O volume de exposição a um comprometimento de CHD ou de CDE
- A probabilidade e a frequência de ameaças à empresa ou seus ativos
- Se o TPSP já esteve envolvido em um comprometimento de dados do titular do cartão

As *Diretrizes de avaliação de risco do PCI DSS* fornecem mais informações para a realização de uma avaliação de risco e podem ser indicadas por entidades que buscam orientação mais detalhada neste processo.

Abaixo encontra-se uma lista de alto nível de algumas das perguntas e tópicos que podem ser apropriados na consideração de parte da avaliação de risco. A lista não é exaustiva e é considerada um ponto de partida para uma empresa usar ao criar seu próprio processo de avaliação de risco:

Governança de segurança e gestão de riscos

- O TPSP tem um programa de segurança da informação implementado que inclui políticas e procedimentos documentados?
- Que tipos de auditorias internas ou externas, se houver, são realizadas nas unidades do TPSP?
- Há outros padrões do PCI ou da indústria que sejam aplicáveis ao ambiente ou ao TPSP?
- O TPSP realiza verificações periódicas de vulnerabilidades e testes de penetração em ativos, aplicativos e sistemas contendo dados do cliente?
- O TPSP reavalia formalmente suas ameaças e riscos à segurança da informação em intervalos regulares, com base na frequência de ameaças emergentes aos seus sistemas e processos? O processo de avaliação é baseado em uma metodologia padronizada de avaliação de risco (indicada no Requisito 12.2⁷ do PCI DSS)?
- O TPSP já teve uma violação de dados?

⁷Esta referência é ao PCI DSS v3.1 – Abril de 2015

Práticas de recursos humanos

- Como as verificações de antecedentes são realizadas em recursos que podem ter acesso às informações do cliente do TPSP? As verificações de antecedentes são repetidas em intervalos predeterminados?
- Como são tratadas as rescisões?
- Existem políticas de não divulgação para proteger a divulgação de informações tanto do TPSP quanto de seus clientes?
- O TPSP tem políticas relativas à transmissão, ao armazenamento e ao processamento de dados confidenciais, bem como a dados de clientes?

Segurança física

- Existe um programa de segurança física em vigor nas unidades do TPSP onde os sistemas ou serviços aplicáveis são fornecidos?

Entidades externas de terceiros

- Alguma entidade externa envolvida pelo TPSP tem acesso às instalações, sistemas ou aplicativos de processamento de dados do TPSP?
- O TPSP realiza a due diligence em entidades externas com as quais se envolve?
- O TPSP monitora a conformidade e o risco de entidades externas com as quais se envolve?

Gerenciamento de configuração

- Existe um processo formal de controle de alterações e gerenciamento de configuração implementado no TPSP?
- O TPSP atualiza patches críticos dentro de um período especificado? Ele tem uma política relativa à gestão de patches?
- O TPSP tem algum hardware ou software que não é mais suportado pelo fabricante (que esteja além de seu fim de vida útil)?
 - Os sistemas e aplicativos são reforçados de acordo com um padrão documentado?
 - O TPSP tem referências de configuração seguras para todas as plataformas que compreendem sua infraestrutura de serviço comum?

Autorização de acesso

- Como é autorizado o acesso lógico e físico aos dados e ativos do cliente?
 - Se os processos de acesso a sistemas forem compartilhados, as funções e responsabilidades são claramente documentadas?
- Como são revisados os direitos para o acesso físico e lógico?
- O TPSP sempre usa uma credencial de autenticação exclusiva (como uma senha/frase) para cada cliente?

Resposta a incidentes

- O TPSP tem um plano de resposta a incidentes?
- O TPSP tem procedimentos para relatar a segurança lógica e física e incidentes de privacidade aos clientes?
- Os procedimentos do TPSP incluem informações de contato para autoridades ou investigadores forenses?

Controles de malware

- Que controles o TPSP tem em vigor para detectar, conter e erradicar vírus, worms, spyware e códigos mal-intencionados?
- Esses controles são implementados em todos os ativos do TPSP que transmitem, armazenam ou processam os dados do titular do cartão da entidade?
- Que tipos de mecanismos de detecção de alterações estão presentes nos sistemas do TPSP?
- O TPSP investiu em algum produto de segurança ou serviços que não seja aquele exigido pelo PCI (antivírus, FIM) que melhoram sua capacidade de detectar malware?

Controles de separação e segurança

- Quais controles estão implementados para manter os sistemas, aplicativos e dados do cliente separados de outros ativos de clientes e inacessíveis a outros clientes ou à rede interna do TPSP?

3.4 Documentação dos resultados

Uma empresa também deve considerar documentar totalmente os resultados de sua pesquisa sobre o TPSP e revisar seu status de conformidade. Além de quaisquer outras informações e materiais considerados necessários ou apropriados através do processo de due diligence, cada entidade realmente deve considerar a captura e inclusão dos seguintes dados críticos, uma vez que cada um deles será inestimável no futuro:

- Data de aniversário – Qual é a data em que a documentação de conformidade vence, exigindo que a revalidação tenha ocorrido?
- Fornecedores de validação de conformidade – Com quais fornecedores e avaliadores de segurança e conformidade o TPSP trabalha? Isso pode incluir QSAs, ASVs que realizam verificações, etc.
- Banco adquirente – Se aplicável, com qual banco adquirente o TPSP trabalha?
- Banco patrocinador – Identifique se o TPSP usa um banco patrocinador para acesso às redes de cartões de pagamento.
- Área auditada – Quais áreas de serviço específicas foram validadas e como elas se alinham aos serviços prestados à entidade?
- Prestadores de serviços integrados – Existem outros TPSPs integrados na conformidade do TPSP? Quais serviços os TPSPs integrados oferecem?
- Documentação de um modelo de responsabilidade compartilhada – A entidade avaliada deve documentar claramente os requisitos do PCI DSS que são gerenciados por cada TPSP e aqueles que são gerenciados pela entidade.

4 Contratação do prestador de serviços terceirizado

Após pesquisar com sucesso um TPSP e concluir a due diligence, a entidade buscará contratar o TPSP. As seções a seguir descrevem as etapas importantes a serem consideradas ao contratar um TPSP.

4.1 Acordo de confidencialidade (Non-Disclosure Agreement, NDA)

Um NDA com TPSPs pode ser prático para sua empresa no processo de pré-seleção e antes de qualquer informação ser compartilhada ou divulgada. Os NDAs neste estágio devem ser simples e concisos, e devem especificar o propósito e os termos da contratação. Para simplificar este processo, recomenda-se que os NDAs sejam elaborados pelo seu departamento jurídico (ou a área que cuida de suas questões jurídicas) antes de contratar quaisquer TPSPs, e garantir que seu departamento jurídico esteja disponível para revisar quaisquer alterações propostas ou ainda para revisar o NDA do TPSP.

4.2 Estabelecer expectativas

Como acontece com qualquer projeto, definir as expectativas de todas as partes envolvidas conduz a uma possibilidade maior de sucesso. Definir expectativas é fundamental para alcançar um modo de operação consistente e acordado.

Além dos outros assuntos determinados como importantes pelas partes, é importante definir, concordar e documentar cada uma das seguintes expectativas no início da contratação e revisar essas expectativas, no mínimo, anualmente e após uma mudança nos serviços, para garantir que o consenso ainda seja mantido.

- A meta fundamental da entidade é entender claramente o status de conformidade do PCI DSS do TPSP e, como resultado, permitir que ele alcance e mantenha sua própria conformidade com o PCI DSS e tenha garantia de que o TPSP está protegendo os dados do titular do cartão da entidade, que se encontram em posse dele, de forma suficiente.
- A responsabilidade do TPSP de proteger os CHD da entidade que se encontram em sua posse de forma suficiente, conforme acordado.
- Os serviços específicos fornecidos pelo TPSP para a entidade.
- Os principais contatos tanto na entidade quanto no TPSP. Com relação a esse ponto, pode ser importante identificar indivíduos específicos, juntamente com o pessoal de apoio, caso o contato principal (point of contact, POC) não esteja disponível. Também é importante documentar informações de contato, incluindo e-mail, telefone comercial e celular. Esses indivíduos (ou outros especificados) devem ser responsabilizados pelas atividades de due diligence, além de assumir responsabilidades de comunicação, abordar incidentes e fornecer informações relacionadas à conformidade.
- A entidade pode querer considerar a inclusão, em sua análise e em um potencial contrato com o TPSP, que este mantém o nível adequado de especialização em segurança e conformidade em relação aos serviços que ele fornece à entidade. Isso pode ser um ponto especialmente crítico para TPSPs de alto risco.

4.3 Obter transparência

Avaliar corretamente o escopo da responsabilidade do TPSP quanto à proteção de CHD ou CDE da entidade é essencial, já que as opiniões de indivíduos e organizações relacionadas ao escopo podem diferir. Para que isso ocorra, a entidade pode querer considerar solicitar a visualização de evidências que comprovem que o escopo é preciso com base no que o TPSP reivindicou. Conforme detalhado na seção 3.2.2, “Documentação de validação do prestador de serviços terceirizado”, essas informações podem ser proprietárias ou confidenciais e podem exigir redação, visualização remota, visualização presencial ou conversas por telefone. Idealmente, um ISA ou um QSA deve revisar as evidências fornecidas para verificar se o escopo é realmente aplicável, apropriado e preciso. Um indivíduo que é bem versado e experiente no projeto e segmentação de rede também pode fornecer esse conhecimento, se um ISA ou QSA não estiver disponível.

As entidades também podem considerar o uso de disposições contratuais adequadas com TPSPs que permitem e exigem o compartilhamento adequado de evidências, para evitar situações em que o TPSP não seja obrigado a facilitar esse processo de compartilhamento de evidências. Se todas as tentativas falharem na obtenção das evidências necessárias do TPSP, a entidade pode considerar solicitar que este documento sua definição de escopo por escrito e inclua uma disposição para que ele retenha a documentação durante o período acordado. Informações adicionais podem ser encontradas na Seção 5, “Acordos por escrito, políticas e procedimentos”.

4.4 Estabelecer comunicações

Uma das chaves para o sucesso na relação entre a entidade e o TPSP é uma comunicação eficaz. Sem uma comunicação eficaz, alterações podem ser feitas pelo TPSP sem o conhecimento ou concordância da entidade, que podem afetar negativamente o status geral de conformidade do PCI DSS da entidade. A determinação de uma mudança significativa varia de entidade para entidade, dependendo do tipo de mudança e do seu impacto.

As comunicações podem ser promovidas e melhoradas estabelecendo-se o cronograma de comunicação como parte do processo de integração para o programa de monitoramento, atribuindo os principais contatos, na entidade e no TPSP, como partes responsáveis em comunicar proativamente assuntos importantes. Se apropriado, esses contatos também podem ser responsáveis pela distribuição adequada de informações dentro das empresas relevantes de forma oportuna, de modo que o risco possa ser mitigado.

O cronograma de comunicação deve ser revisado e atualizado anualmente ou conforme necessário, dependendo do tipo e do impacto das alterações. Os seguintes tópicos (lista não exaustiva) podem precisar ser comunicados sempre que ocorrerem alterações e/ou anualmente, conforme aplicável.

- Alterações no CDE
- Alterações na estrutura de processamento de pagamento da entidade ou do TPSP
- Alterações na equipe responsável por manter as operações com o TPSP e a entidade
- Alterações na equipe envolvida com a iniciativa de due diligence
- Alterações nos processos, procedimentos e metodologias que afetam o CDE
- Todas as outras instâncias em que uma atividade afetará o escopo da entidade

4.5 Solicitar evidência

Além das evidências solicitadas para apoiar os serviços e o escopo fornecidos pelo TPSP, a entidade pode precisar verificar se os procedimentos apropriados foram seguidos e se os controles para apoiar as mudanças foram implantados. Para isso, a entidade pode determinar que é apropriado solicitar evidências de apoio sempre que receber uma comunicação do TPSP e avaliar o risco a ser aplicável. Consulte a seção 4.3 “Obter transparência” acima para informações sobre os materiais e métodos de comunicação aplicáveis.

Se a própria entidade avaliará o status de conformidade do PCI DSS do TPSP, ou seja, a entidade empregará os serviços de um de seus ISAs ou um QSA externo para determinar a conformidade do TPSP, pode ser apropriado solicitar evidências anualmente de forma a apoiar a avaliação do PCI DSS.

4.6 Obter informações sobre a conformidade do PCI DSS

A Seção 3.2.2, “Documentação de validação do prestador de serviços terceirizado”, fornece exemplos das informações que podem ser obtidas de um TPSP em relação ao seu status de conformidade, se o TPSP foi validado ou se não é necessária a validação. É opcional às entidades executar uma avaliação de conformidade do PCI DSS dos serviços aplicáveis fornecidos pelo TPSP ao empregar os serviços de um dos seus ISAs próprios ou de um QSA externo. Essa avaliação do PCI DSS deve, preferencialmente, ser realizada no início da contratação. No entanto, realizar a avaliação após o início da contratação ainda pode fornecer informações e uma referência a partir da qual trabalhar. Em seguida, pode-se realizar avaliações anuais que preferencialmente terminem alguns meses antes da data de avaliação do PCI DSS da entidade para permitir qualquer resolução que seja necessária.

Como acontece com as armadilhas detalhadas na seção 4.3, “Obter transparência”, acima, a eficácia na realização desse tipo de avaliação depende da disposição do TPSP de fornecer as informações necessárias. Dependendo dos acordos legais entre as partes, pode haver muitos casos em que o TPSP negue o fornecimento de informações proprietárias e confidenciais. Conforme detalhado em “Obter transparência”, a entidade pode desejar solicitar que o TPSP documente sua recusa em fornecer as informações por escrito, se apropriado.

4.7 Frequência da revisão

A tabela a seguir mostra a frequência sugerida para revisão das etapas da contratação:

Contratação de prestadores de serviços terceirizados			
Etapas	Inicialmente	Conforme ocorrerem alterações*	Anualmente
▪ Estabelecer expectativas	X	X	X
▪ Obter transparência	X	X	X
▪ Estabelecer comunicações	X	X	X
▪ Solicitar evidência	X	X	X
▪ Obter informações sobre a conformidade do PCI DSS	X		X

****Observação:** dependendo do tipo de alteração introduzida, esta etapa pode ou não ser necessária. Por exemplo, uma mudança significativa na infraestrutura pode iniciar todas as etapas, enquanto uma mudança que não afeta a conformidade com o CDE ou o PCI DSS - por exemplo, alterações no contato principal - pode acionar apenas algumas delas. O resultado das avaliações de risco realizadas durante o processo de due diligence ajudará a determinar com que frequência essas*

4.8 Mapeamento de serviços de terceiros para os requisitos aplicáveis do PCI DSS

É fundamental que a entidade compreenda totalmente como os serviços e produtos fornecidos são mapeados pelo TPSP quanto aos requisitos do PCI DSS para que esta possa determinar o impacto da segurança no ambiente de dados do titular do cartão.

Os requisitos aplicáveis a um TPSP variam dependendo de diversos fatores, incluindo a natureza dos serviços prestados, o nível de acesso que ele tem ao CDE, entre outros. Por exemplo, um TPSP que fornece serviços de gerenciamento de firewall pode ter de atender ao Requisito 1⁸ do PCI DSS. Um TPSP que fornece serviços de manutenção que incluem acesso incidental ao CDE pode exigir verificações de antecedentes e/ou acompanhamento em áreas sensíveis.

O Anexo A deste documento fornece uma tabela que mostra sugestões e pontos de discussão que podem ajudar a esclarecer e determinar como as responsabilidades para manter os requisitos do PCI DSS podem ser compartilhadas entre a entidade e o TPSP. **O Anexo B** é um exemplo da Matriz de responsabilidades do PCI DSS para ajudar uma entidade a começar a compreender como os requisitos do PCI DSS podem ser mapeados para os serviços que uma entidade terceiriza para um TPSP e a responsabilidade relacionada a cada um deles.

⁸Esta referência é ao PCI DSS v3.1 – Abril de 2015

5 Acordos por escrito, políticas e procedimentos

Observação: as informações e orientações fornecidas nesta seção e, em geral, ao longo deste Suplemento de informações, não constituem qualquer consultoria jurídica e, conseqüentemente, não devem ser consideradas ou interpretadas como tal. As entidades que buscam contratar um TPSP para realizar serviços são realmente incentivadas a buscar orientação jurídica de um profissional devidamente qualificado para garantir que cada parte compreenda plenamente seus direitos e obrigações, e que as expectativas das partes estejam alinhadas. Entidades com perguntas específicas sobre assuntos legais devem consultar um profissional da área jurídica devidamente qualificado. As informações e orientações fornecidas nesta seção não substituem as leis locais ou regionais, regulamentos governamentais ou outros requisitos legais. Por fim, os termos específicos do acordo entre uma entidade e um TPSP devem refletir todos os detalhes dos serviços que são fornecidos e os direitos e responsabilidades relevantes de ambas as partes.

Uma vez que um processo de avaliação de risco apropriado tenha sido concluído e um TPSP tenha sido selecionado para uma contratação, a melhor prática sugere que a entidade e o TPSP documentem seu acordo por escrito. A discussão abaixo tem como objetivo destacar certas questões específicas para uma relação típica entre entidade e TPSP que a entidade pode querer considerar ao buscar contratar um TPSP. Entidades com acordos existentes com TPSPs também podem considerar o seguinte ao analisar esses acordos. O que se segue não tem a intenção de ser uma lista exaustiva e é fornecido visando à conveniência para ajudar a familiarizar as entidades que buscam contratações de TPSPs com os tipos de problemas que comumente surgem neste contexto. Outros problemas podem surgir e ser igualmente ou mais importantes, e as entidades são realmente incentivadas a buscar uma assessoria jurídica devidamente qualificada em conexão com todos os acordos comerciais.

5.1 Acordos entre prestadores de serviços terceirizados em conformidade com o PCI DSS em comparação a prestadores de serviços terceirizados sem conformidade com o PCI DSS

Os TPSPs que passaram pela avaliação de conformidade do PCI DSS e são validados como estando em conformidade:

Ao contratar um TPSP que afirma que seus serviços estão em conformidade com o PCI DSS, as entidades devem considerar documentar essa conformidade. A documentação específica que pode ser fornecida dependerá, em última instância, da situação e do acordo entre as partes, e poderá incluir uma disposição para um AOC, SAQ e/ou seções relevantes do ROC (redigidas para proteger qualquer informação confidencial), incluindo:

- Data da avaliação de conformidade
- Componentes do sistema, serviços e ambientes incluídos na avaliação do PCI DSS de terceiros
- Componentes do sistema e serviços que foram excluídos da avaliação do PCI DSS, conforme aplicável aos serviços fornecidos

Ter os recursos do TPSP disponíveis (incluindo o ISA ou QSA, se necessário) para responder a quaisquer perguntas de esclarecimento pode ser útil para validar que os serviços fornecidos pelo TPSP estão cobertos. Da mesma forma, as disposições que reconhecem as respectivas responsabilidades das partes em processar e proteger os CHD em sua posse, em conformidade com o PCI DSS, podem auxiliar na

validação. Rastrear a frequência da validação de conformidade também pode ajudar na gestão e monitoramento do TPSP conforme exigido pelo Requisito 12.8 do PCI DSS⁹.

TPSPs que não passaram por uma avaliação ou não têm necessidade de validação da conformidade com o PCI DSS:

Uma entidade que é obrigada a estabelecer a conformidade com o PCI DSS e que utilize os serviços de um TPSP que não estabeleceu, afirmativamente, sua própria conformidade com o PCI DSS pode precisar abranger alguns ou todos os ambientes do TPSP como parte de suas próprias avaliações do PCI DSS. Mais especificamente, a avaliação do PCI DSS de uma entidade precisará abranger qualquer serviço do TPSP que exija (ou possa possibilitar ou permitir) que o TPSP processe CHD ou que possa afetar a segurança do CDE. Como resultado, entidades que buscam contratar TPSPs neste contexto podem querer considerar mecanismos (como a capacidade de auditar o TPSP) destinados a ajudar a promover a transparência e auxiliar no processo de validação da conformidade do PCI DSS, como:

- Acesso a sistemas, instalações e pessoal apropriado para revisões no local, entrevistas, vistorias físicas, etc.
- Revisão das políticas, procedimentos, documentação do processo, padrões de configuração, registros de treinamento, planos de resposta a incidentes, etc. do TPSP que evidenciem o cumprimento dos requisitos aplicáveis do PCI DSS e/ou que o TPSP cumpra com a política da entidade.
- Revisão de evidências (como configurações, capturas de tela, revisões de processo, etc.) para auxiliar na validação de que todos os requisitos aplicáveis do PCI DSS estão sendo atendidos quanto aos componentes do sistema dentro do escopo do ambiente do TPSP.
- Clareza com relação às partes do ambiente do comerciante gerenciadas pelo TPSP que estão dentro do escopo da avaliação do PCI DSS da entidade/comerciante.
- Retenção de evidências coletadas em função da não conformidade
- Alocação de responsabilidade para processar e proteger os dados do titular do cartão em conformidade com o PCI DSS.
- Frequência da validação/avaliação de conformidade do PCI DSS (por exemplo, anualmente, trimestralmente, etc.).

5.2 Considerações ao estabelecer acordos, políticas e procedimentos

Requisitos regulatórios regionais

Recomenda-se que uma entidade avalie todos os requisitos regionais (por exemplo, nacional, estadual, regional, municipal) que possam ser aplicáveis. Por exemplo, alguns comerciantes, como agências estaduais ou universidades públicas, podem ser obrigados a cumprir requisitos estaduais específicos com relação a questões específicas (como dependência do ciclo orçamentário para pagamento) ou seleção de um TPSP. Uma entidade deve consultar as agências federais, regionais, estaduais (por exemplo, controlador estadual), locais e estrangeiras para determinar as limitações e diretrizes aplicáveis.

⁹ Esta referência é ao PCI DSS v3.1 – Abril de 2015

Considerações legislativas

Uma entidade pode querer consultar as leis aplicáveis que podem conter disposições adicionais sobre:

- Definições de informações confidenciais ou protegidas
- Limites de notificação de violação
- Requisitos específicos de proteção contra roubo de identidade
- Requisitos de proteção aprimorados para categorias específicas de dados confidenciais ou outros

Essas disposições podem variar de acordo com a política ou acordo típico da entidade. A entidade deve buscar orientação jurídica em relação a todos os requisitos legais, regulatórios e outros requisitos aplicáveis para cada jurisdição, área e região em que estará operando. O valor de entender e alocar a responsabilidade pelo cumprimento de todos esses requisitos não pode ser subestimado, especialmente nos locais em que se encontram os ambientes de pagamento físico e virtual.

Considerações do adquirente

Cada adquirente pode ter seus próprios requisitos relacionados à contratação de um TPSP. Uma entidade pode querer revisar seus acordos com adquirentes para garantir que seus TPSPs (ou os TPSPs dos adquirentes) cumpram quaisquer responsabilidades específicas do adquirente em relação a TPSPs.

Considerações sobre a bandeira do cartão de pagamento

Cada bandeira de cartão de pagamento criou seus próprios programas de conformidade. As entidades que buscam contratar TPSPs devem levar em consideração a análise desses requisitos do programa de conformidade com os TPSPs para identificar e alocar adequadamente as responsabilidades correspondentes, e para garantir que cada um compreenda e cumpra com todos os termos aplicáveis da bandeira de cartão de pagamento.

Considerações específicas da indústria

Em várias indústrias e verticais, existem regulamentos e requisitos específicos que as entidades podem levar em consideração, já que podem ser importantes para o relacionamento e a alocação de direitos e responsabilidades entre uma entidade e um TPSP. Questões específicas a serem consideradas podem incluir o manuseio de equipamentos que fazem parte do CDE, requisitos de destruição de dados e níveis de proteção necessários para atender aos requisitos de conformidade. Uma entidade e um TPSP devem discutir quaisquer requisitos específicos do setor que possam ser pertinentes.

Considerações específicas da política interna (relações com subsidiárias)

Caso uma empresa controladora e sua subsidiária estabeleçam um relacionamento em que uma é um TPSP e a outra estiver utilizando os serviços do TPSP, questões adicionais a serem consideradas podem incluir:

- O TPSP está incorporando subsidiárias em sua avaliação do PCI DSS ou está realizando avaliações separadas do PCI DSS entre essas subsidiárias?
- O TPSP é considerado um prestador de serviços/comerciante com um nível diferente da entidade? Isso afeta o tipo de validação que qualquer um deles deve realizar?

- O que o TPSP realmente fornece à entidade?
- Quais outros aspectos dos relacionamentos podem ser relevantes (por exemplo, franqueado independente versus franqueado corporativo)?

Observação: há um alto grau de variabilidade na formalização de acordos contratuais entre empresas controladoras e subsidiárias. Esses acordos variam de contratos verbais, acordos de nível de serviço internos informais até sofisticados contratos entre partes independentes. No entanto, possíveis problemas e preocupações

5.3 Considerações adicionais

Entidades que buscam contratar TPSPs também podem considerar o seguinte.

5.3.1 Matriz de responsabilidades

Uma matriz de responsabilidades normalmente é um cronograma ou anexo que detalha as responsabilidades específicas das partes em um acordo, em um formato tabular fácil de entender. Uma matriz de responsabilidades, no contexto entre a entidade e o TPSP, pode ser útil para ajudar a identificar uma variedade de problemas, incluindo, entre outros, responsabilidades, procedimentos e prazos de notificação para os seguintes itens:

Tecnologia

- Compra de componentes do sistema
- Desenvolvimento de componentes do sistema
- Testes/implantação
- Sustentação/manutenção (ou seja, fornecimento de patches, vulnerabilidade e testes de penetração)
- Ciclo de vida do produto ou tecnologia

Processos

- Procedimentos operacionais
- Requisitos de notificação
- Política substituta (em caso de discrepância, qual política será considerada válida)
- Relatórios
- Procedimentos de auditoria que incluem sistemas e instalações, conforme necessário
- Atividades de validação do PCI DSS
- Acesso a sistemas/dados para validação periódica, se necessário (reconciliação de contas, registros, etc.)
- Acesso a sistemas/dados para investigação forense
- Retenção e destruição de dados/evidências
- Recuperação e continuidade dos negócios

Além disso, pode ser apropriado (embora não exigido pelo PCI DSS) definir as responsabilidades conforme a necessidade. Consulte o Anexo B para obter um exemplo.

5.3.2 Violações de dados

Conforme descrito no Requisito 12.10 do PCI DSS¹⁰ em relação ao plano de resposta a incidentes podem ser necessárias várias ações específicas em conexão com suspeitas de violações de dados, dentro de um período muito curto dessa violação. As entidades podem querer considerar a melhor forma de garantir que o TPSP esteja ciente desses requisitos e desenvolver um fluxo de trabalho estabelecendo quando, como e quem um TPSP deve notificar em caso de suspeita de violação de dados. Além do plano de resposta a incidentes exigido pelo PCI DSS, as bandeiras de cartão de pagamento e as leis nacionais ou regionais podem exigir notificação de violação. As entidades devem considerar cada um desses problemas com os respectivos TPSPs e como alocar a responsabilidade para todos os requisitos de notificação aplicáveis e todas as ações de acompanhamento necessárias. As entidades também são realmente incentivadas a incluir em seu contrato com os TPSPs que, em caso de uma violação/comprometimento, os TPSPs devem participar integralmente com o investigador forense do PCI (PFI) e na investigação forense em si, incluindo a disponibilização dos dados, sistemas, componentes e serviços relacionados da entidade para esse fim.

Considerações adicionais podem incluir questões como:

- Etapas esperadas de entidades e/ou TPSPs se houver perda de dados
- Uso de ferramentas como recuperação de arquivos
- Aplicabilidade e adequação da cobertura do seguro
- Responsabilidade pela emissão de notificações
- Responsabilidade financeira pelos custos de notificação
- Prazos de notificação
- Envolvimento de investigadores forenses e responsabilidade pelos custos da investigação
- Documentação clara dos requisitos de relatório de resposta a incidentes (envolvendo dados do titular do cartão), incluindo quem é responsável por notificar o adquirente ou as bandeiras do cartão em caso de um incidente de terceiros

5.3.3 Considerações pós-rescisão sobre TPSPs e seus clientes

Entidades que (a) estão sujeitas a requisitos referentes a CHD ou qualquer CDE (seja orientado pelo PCI DSS, por considerações legais ou de outra forma) e (b) responsabilidades de terceirização relacionadas ao TPSP também podem querer considerar como esses requisitos e responsabilidades podem se aplicar ao TPSP **depois** da rescisão formal da contratação entre entidade e TPSP. Por exemplo, se um TPSP continuar a armazenar os CHD de uma entidade como parte de um sistema de backup de arquivo, as obrigações correspondentes do TPSP, relativas a esses CHD, também podem continuar. Como resultado, a entidade pode querer considerar se o relatório pós-rescisão, as notificações, a retenção de dados ou os requisitos relacionados são apropriados e/ou se uma notificação deve ser fornecida (mesmo após o encerramento do relacionamento entre entidades TPSP) caso o TPSP destrua ou remova irreversivelmente os dados de suas instalações e/ou dispositivos.

Considerações semelhantes surgem em conexão com os funcionários rescindidos do TPSP. Se um indivíduo puder ter acesso às informações confidenciais da entidade (incluindo CHD ou CDE) durante a vigência do seu contrato de trabalho com o TPSP, as entidades e os TPSPs podem querer

¹⁰ Esta referência é ao PCI DSS v3.1 – Abril de 2015

considerar mecanismos para ajudar a garantir que essas informações sejam protegidas após a relação trabalhista terminar, como:

- Obrigações contínuas de confidencialidade após a rescisão
- Alocação apropriada de responsabilidade para garantir a conformidade pelos funcionários do TPSP com suas obrigações de confidencialidade contínuas
- Alocação apropriada de responsabilidade pela execução de obrigações de confidencialidade e pelos custos associados à execução e aos respectivos processos legais, em caso de descumprimento dessas obrigações
- Cessação do acesso dos funcionários do TPSP aos edifícios ou sistemas imediatamente após a rescisão do contrato de trabalho

5.3.4 Terceirização da funcionalidade fornecida (TPSPs integrados)

Se o TPSP terceirizar uma parte dos serviços que ele concordou em fornecer à entidade através de outro prestador de serviços, todas as questões e preocupações mencionadas acima também se aplicam ao relacionamento entre o TPSP e o prestador terceirizado. Isso, por sua vez, pode afetar o escopo do CDE da entidade e, por fim, o escopo da validação do PCI DSS da entidade. Como resultado, para ajudar a gerenciar essas complexidades e riscos relacionados, as entidades podem querer considerar se mecanismos, como os a seguir, podem ser apropriados:

- Uma notificação para a entidade quanto à ocorrência da terceirização
 - O TPSP, que foi inicialmente contratado para fornecer serviços à entidade que busca conformidade com o PCI, deve fornecer informações relacionadas a outros terceiros (por exemplo, TPSPs integrados) que serão envolvidos no apoio à entidade, como parte da documentação inicial de contratação.
- Limitações apropriadas com relação à terceirização de funcionalidades, como exclusões regionais devido a questões jurisdicionais
 - A entidade que busca um TPSP para terceirização de serviços que poderia afetar a segurança do ambiente de dados do titular do cartão deve estabelecer procedimentos documentados para a inclusão de cláusulas com limitações e exclusões detalhadas, dependendo do tipo de serviços a serem terceirizados e preocupações com conformidade jurisdicional e regulatória (por exemplo, leis de proteção de dados no país, normas de privacidade, etc.), evitando declarações de responsabilidade geral e voltando-se mais para a singularidade dos riscos inerentes associados aos serviços a serem terceirizados.
- Alocação apropriada de passivos, responsabilidades e custos relacionados a ações de prestadores terceirizados e/ou notificação à entidade sobre incidentes

Embora a obrigação da entidade de cumprir o Requisito 12.8.4¹¹ se estenda apenas ao monitoramento e coleta de evidências do status de conformidade de seus TPSPs contratados diretamente, a entidade também pode querer analisar, cuidadosamente, a confiança e a supervisão contínua que seus TPSPs têm sobre quaisquer TPSPs integrados.

¹¹ Esta referência é ao PCI DSS v3.1 – Abril de 2015

5.3.5 Perda do status de conformidade

A perda do status de conformidade do PCI DSS por um TPSP pode ter ramificações significativas para uma entidade que depende dos serviços do TPSP. Consequentemente, as entidades podem querer considerar mecanismos destinados a mantê-las informadas das alterações no status de conformidade do PCI DSS e alocar adequadamente a responsabilidade pela perda do status de conformidade entre as partes. Esses mecanismos podem incluir:

- A divulgação/notificação de alterações no status de conformidade para a entidade impactada
- Planos e procedimentos de resolução para restabelecer a conformidade segundo as datas estabelecidas
- Reuniões regulares de status para aconselhar sobre os esforços de resolução
- Outras medidas apropriadas destinadas a ajudar a garantir a prestação de contas e a responsabilidade pela não conformidade

6 Manutenção de relacionamentos e monitoramento de prestadores de serviços terceirizados

Criar e manter um programa para monitorar a conformidade do TPSP com o Requisito 12.8.4 do PCI DSS¹² é uma exigência crítica para qualquer entidade. Um programa de monitoramento permitirá que uma entidade monitore o status de conformidade do(s) TPSP(s) e determine se uma mudança no status requer uma alteração no relacionamento. A validação da conformidade ocorre em um momento determinado e, infelizmente, é muito fácil para uma entidade permitir haja um relaxamento em relação aos processos e que a conformidade seja negligenciada. Contar com outras partes para a prestação de serviços — incluindo a terceirização de funções críticas — não isenta uma entidade da responsabilidade pela segurança dos dados do titular do cartão, e a conformidade do TPSP deve ser monitorada contínua e diligentemente.

Investir o tempo e o esforço necessários para desenvolver e implementar um programa sólido de monitoramento TPSP oferece inúmeros benefícios para a entidade. Primeiro e mais importante, o programa de monitoramento melhorará a postura de segurança da entidade e ajudará a garantir a proteção dos dados do titular do cartão pelos quais a organização é responsável ao fornecer garantia e conscientização sobre se o TPSP continua a compartilhar o mesmo nível de compromisso no processamento de CHD. Um programa de monitoramento também garantirá que haja comunicação regular entre o TPSP e a entidade com relação a alterações no ambiente, incluindo processos e procedimentos. Isso permite que a entidade esteja em uma posição proativa, em vez de reativa. Em segundo lugar, o programa de monitoramento fornecerá um processo consistente para simplificar o monitoramento e o gerenciamento contínuos dos TPSPs. Por fim, o programa de monitoramento permitirá que uma entidade demonstre a conformidade com uma seção fundamental do PCI DSS, caso seja solicitada comprovação de uma parte que esteja realizando uma avaliação.

Como parte do programa de monitoramento de uma entidade, um processo de integração para novos TPSPs deve ser desenvolvido e mantido, incluindo o fornecimento de informações obtidas através dos vários estágios da contratação (ou seja, análise de risco, detalhes do contrato, matriz de responsabilidades etc.) aos novos TPSPs. Essas informações adicionais devem ser incorporadas no programa de monitoramento para criar a estrutura para monitoramento de um TPSP.

6.1 Desenvolvimento de um programa de monitoramento de prestadores de serviços terceirizados

O programa de monitoramento do TPSP deve ser totalmente documentado. Isso garante que haja um entendimento comum de seus elementos em toda a organização, facilita a delegação de partes do processo, se exigido, e também permite a revisão do processo por parte de terceiros, quando necessário. Os elementos do programa devem incluir processos, políticas e procedimentos, e a atribuição de responsabilidade a pessoas específicas dentro da organização para esses elementos. A documentação do programa deve ser revisada regularmente para fazer correções e melhorias à medida que os processos comerciais e as relações do TPSP evoluem. Recomenda-se que a documentação do programa seja revisada pelo menos uma vez ao ano e aprovada pela gerência.

A documentação do programa deve abranger as seguintes áreas, incluindo orientação sobre seu objetivo e sua importância:

¹² Esta referência é ao PCI DSS v3.1 – Abril de 2015

6.1.1 Definição do escopo do ambiente de dados do titular do cartão (Cardholder Data Environment, CDE)

Garantir que o escopo do CDE esteja corretamente definido e verificado é fundamental para determinar o nível de esforço necessário para se alcançar a conformidade. A entidade precisa garantir que todos os recursos envolvidos no monitoramento de TPSPs entendam o conceito de escopo do CDE e precisa especificar o que é necessário para definir completamente o escopo (por exemplo, um diagrama de rede de alto nível com aplicativos e componentes de rede claramente rotulados, atividades de validação fora do escopo, etc.). Uma vez confirmado o escopo, o programa deve incluir um resultado que explique o escopo do CDE e indique o papel de cada TPSP e como ele impacta o escopo do PCI DSS da entidade.

6.1.2 Manutenção de um inventário de prestadores serviços terceirizados

Definir os procedimentos para manter um inventário de todos os TPSPs, incluindo os elementos de informação considerados críticos. Os elementos sugeridos a seguir podem ser incluídos no inventário:

- Nome e contatos principais no TPSP
- Serviços específicos fornecidos
- Se os dados do titular do cartão forem compartilhados, quais elementos serão compartilhados (dados de autenticação confidenciais, PAN, validade, etc.)
- Localização dos dados — são os dados armazenados internamente na empresa, por terceiros em uma de suas unidades ou por um provedor de hospedagem externo
- Quais componentes do sistema estão incluídos na revisão
- Resultados da avaliação de riscos do TPSP
- Frequência do ciclo de monitoramento
- Data da última revisão
- Renovação/vencimento do contrato
- Documentação/evidência necessárias
- Todos os TPSPs integrados utilizados para fornecer os serviços
- Quaisquer aplicativos de pagamento de terceiros usados para fornecer os serviços
- Volume de dados do titular do cartão que são armazenados/processados/transmitidos/afetados pelo TPSP
- Acesso lógico à rede da entidade
- Quaisquer designações que o TPSP possua que ofereçam suporte ao seu atestado de conformidade do PCI DSS (ISO, PCI QIR, PCI PTS, FIPS 140 etc.)

6.1.3 Procedimento para monitoramento de prestador de serviços terceirizado

Abaixo há uma descrição de alto nível dos componentes que uma entidade pode querer levar em consideração, inclusive quanto ao seu procedimento de monitoramento de TPSP. A lista não é exaustiva e não tem por objetivo definir o único método de monitoramento do status de conformidade do PCI DSS do TPSPs. Entretanto, a lista descreve alguns componentes recomendados que podem ser incluídos no procedimento.

6.1.3.1 Documentação/evidência

Definir a evidência e documentação comprobatória que serão coletadas dos TPSPs para análise e retenção. Conforme especificado anteriormente, uma informação fundamental a ser coletada é o papel do TPSP no CDE. Essa informação pode estar disponível nas seções aplicáveis do ROC ou na Parte 2E, “Descrição do ambiente no AOC”. Consulte a seção 3.2.2, “Documentação de validação do prestador de serviços terceirizado” para obter informações adicionais.

6.1.3.2 Análise do status de conformidade do PCI DSS do prestador de serviços terceirizado

Descrever o processo de análise do status de conformidade do PCI DSS em detalhes, incluindo elementos de informações específicos a serem examinados. Em particular, é importante que os analistas comparem os processos auditados como parte da avaliação do TPSP aos serviços prestados à empresa. Descrever quaisquer riscos inerentes ao uso de serviços que não foram incluídos na avaliação. Desenvolver uma lista de verificação para ajudar o analista. Se possível, esses critérios devem ser discutidos e revisados anualmente se houver mudança no nível ou tipo de serviço.

6.1.3.3 Descrição de resultados

Desenvolver uma especificação de relatório — ou até mesmo um modelo de relatório — para ajudar o analista a documentar os resultados da análise do status de conformidade do PCI DSS do TPSP. Considerando que analistas diferentes na organização participam do processo, a documentação deve ser elaborada de forma muito consistente para que eles gerem resultados semelhantes. A descrição pode incluir a data de aniversário, fornecedores de validação de conformidade, banco adquirente, banco patrocinador e áreas auditadas.

6.1.3.4 Acompanhamento da revisão

Especificar como os resultados da análise do status de conformidade do PCI DSS do TPSP devem ser compartilhados e aprovados internamente. Determinar as etapas e os prazos para compartilhar resultados com o TPSP analisado e estabelecer expectativas com o TPSP, se um trabalho adicional for necessário. Descrever os procedimentos de encaminhamento que devem ser realizados se um TPSP se enquadrar em um status de não conformidade ou se recusar a obter ou provar a conformidade com o PCI DSS ou se não for necessária a validação quanto à conformidade com o PCI DSS.

6.1.3.5 Controle de acesso e retenção de dados

Definir políticas para monitoramento e controle de resultados do programa (por exemplo, documentação comprobatória, evidências e relatórios de resultados) durante a geração e armazenamento subsequente. Definir uma política específica para retenção de dados do programa de monitoramento. Recomenda-se que a documentação seja mantida por um período mínimo de 3 (três) anos consecutivos.

6.2 Outras considerações

Observação: a seção a seguir pode ser usada como guia sobre sugestões de como proceder em um cenário específico. Essas ações podem ter consequências imprevistas e devem ser cuidadosamente analisadas quanto ao impacto

6.2.1 O prestador de serviços terceirizado não fornece as informações solicitadas

Se um TPSP não responder, não puder ou se recusar a fornecer as informações solicitadas, considere as seguintes ações:

- Garantir que todas as tentativas de comunicação sejam documentadas
- Tentar obter uma explicação do TPSP: Estão sendo solicitadas muitas informações?

Observação: o AOC e/ou as respectivas seções do ROC podem ser suficientes para demonstrar o escopo da avaliação e verificar seu status de conformidade. Outra opção para verificar o status de conformidade do TPSP pode ser ver a documentação na unidade do TPSP ou remotamente, através de uma sessão

- Se o TPSP tiver um banco adquirente, entre em contato com esse banco e solicite assistência com o TPSP para obter as informações necessárias.
- Se todas as tentativas de obter os dados solicitados falharem, pode ser apropriado envolver as bandeiras de cartão de pagamento.
- Se os requisitos de envio do PCI DSS forem documentados no contrato ou acordo com o TPSP, notifique o TPSP da aplicação dos termos do acordo.
- Se todas as outras tentativas falharem, anote nas seções relevantes do ROC na Seção 4.8¹³, “Prestadores de serviços e outras entidades com os quais a empresa compartilha dados do titular do cartão”, que os serviços fornecidos pelo TPSP não puderam ser verificados devido à não comunicação e não cooperação.
- Anote os desafios do TPSP na documentação do programa de monitoramento e aumente o nível de risco do TPSP até o próximo ciclo de revisão.

6.2.2 O prestador de serviços terceirizado não validou a conformidade do PCI DSS

Se um TPSP não estiver avançando com sua conformidade com o PCI DSS, tiver negligenciado sua conformidade ou não pretenda validar ou não tenha necessidade de validar a conformidade do PCI DSS, considere as seguintes ações:

- Converse com o TPSP para determinar a lacuna na conformidade (por exemplo, quais requisitos do PCI DSS não foram atendidos, quais sistemas e/ou processos não estavam em conformidade, quais serviços não foram validados, etc.).
- Solicite evidência do TPSP para comprovar que os requisitos aplicáveis do PCI DSS estão sendo atendidos em relação aos serviços exigidos, conforme detalhado na Seção 3.2.2, “Documentação de validação do prestador de serviços terceirizado”, relacionada aos TPSPs que não validaram a conformidade com o PCI DSS.

¹³ Refere-se à revisão 1.0 – Abril de 2015

- Se o TPSP tiver sido submetido a uma avaliação e tiver enviado a documentação para a validação do PCI DSS às bandeiras de cartão de pagamento e as listas ainda não tiverem sido atualizadas, solicite uma cópia das evidências enviadas para verificar se os requisitos aplicáveis do PCI DSS estão sendo atendidos pelos serviços prestados.
- Se necessário, notifique o banco adquirente da situação e discuta se o adquirente tem etapas específicas para mitigar o risco (por exemplo, plano de ação, atividades de resolução).
- Se o TPSP ainda não tiver concluído a conformidade com o PCI DSS, peça um plano detalhado com prazos para finalizar o processo de conformidade do PCI DSS; certifique-se de que o TPSP forneça verificações de status regularmente, até que atinja a conformidade com o PCI DSS.
- Discuta com o TPSP a frequência para verificar as atividades de conformidade do PCI DSS; recomenda-se de 30 a 60 dias antes do prazo anual de avaliação do PCI DSS.
- Garanta que contratos futuros com TPSPs sejam desenvolvidos levando as diretrizes inseridas neste documento em consideração e entenda as posições e requisitos da empresa relacionados à conformidade do PCI DSS, à medida que novos candidatos TPSP forem entrevistados.
- Informe o TPSP sobre qualquer requisito quanto a um período de notificação para quaisquer alterações ou suporte do serviço, de forma a permitir que haja tempo hábil para uma avaliação de risco a fim de determinar se a mudança afetará a conformidade com o PCI DSS ou os requisitos aplicáveis do PCI DSS.
- Notifique qualquer TPSP que não tenha necessidade de validação quanto à conformidade do PCI DSS de que alterações nos requisitos do PCI DSS, termos da bandeira de cartão de pagamento ou alterações críticas que alterem o relacionamento com o TPSP podem resultar na exigência para que o TPSP valide a conformidade do PCI DSS.
- Se não for possível obter evidências do TPSP para verificar se os requisitos aplicáveis do PCI DSS estão sendo cumpridos, o ambiente e os componentes do sistema do TPSP que fornecem os serviços para a entidade podem precisar ser analisados como parte da revisão anual da avaliação do PCI DSS da entidade e podem estar sujeitos a esforços de resolução para atender à conformidade do PCI DSS. Nas respectivas seções do ROC, na Seção 4.8¹⁴, “Prestadores de serviços e outros terceiros com os quais a entidade compartilha dados do titular do cartão” e com o requisito do PCI DSS aplicável, anote os serviços do TPSP que fazem parte da avaliação.
- Anote os desafios do TPSP na documentação do programa de monitoramento e considere qualquer alteração correspondente no nível de risco atribuído ao TPSP até o próximo ciclo de revisão.
- Se os requisitos de validação do PCI DSS forem documentados no contrato ou acordo com o TPSP, notifique o TPSP da aplicação dos termos do acordo.

6.2.3 O prestador de serviços de terceiros valida a conformidade do PCI DSS através da inclusão na avaliação do PCI DSS da entidade

É possível incluir um serviço do TPSP dentro do escopo do CDE da entidade. Deve-se levar em conta as seguintes considerações para a inclusão:

- Confirme se esta situação é aceitável para o adquirente e/ou bandeira de cartão de pagamento.

¹⁴ Refere-se à revisão 1.0 – Abril de 2015

- Identifique sistemas e processos a serem incluídos na avaliação do PCI DSS da entidade.
- Certifique-se de que o TPSP seja informado sobre as expectativas de melhorias do serviço e da sua sustentabilidade.
- Informe o TPSP sobre qualquer requisito quanto a um período de notificação para qualquer alteração ou suporte do serviço, de forma a permitir uma avaliação para determinar se estes afetarão a conformidade.
- O TPSP deve estar ciente e entender que, uma vez incluídas como parte da avaliação de conformidade da entidade, as mudanças em seus negócios podem afetar adversamente o status de conformidade da entidade.
- Defina claramente os requisitos de “direito de realizar auditoria”, incluindo prazos e o responsável pelos custos incorridos se o comerciante estiver avaliando o TPSP, em vez de confiar em um AOC ou em outra forma de evidência de conformidade do terceiro.

6.2.4 O serviço ou processo existente ou novo não é compatível com PCI DSS ou fará com que a entidade ou TPSP não estejam em conformidade com o PCI DSS

É fundamental manter a conscientização dentro da indústria de cartões de pagamento de que existem várias entidades que não estão em conformidade e que estão trabalhando para se tornar compatíveis com o PCI DSS, e que essas entidades atingirão sua própria conformidade em diferentes momentos, dependendo da complexidade do respectivo CDE. A diferença no status de conformidade pode acarretar uma situação na qual uma entidade ou um TPSP que esteja em conformidade com o PCI DSS seja contratado por uma entidade ou TPSP fora de conformidade, que esteja trabalhando ativamente para cumprir com o PCI DSS.

Se houver um processo ou serviço compartilhado fora da conformidade que não tenha sido abordado anteriormente, seria adequado que os acordos entre a entidade e o TPSP detalhassem se estes são responsáveis pelos requisitos aplicáveis do PCI DSS. No entanto, existe a possibilidade de, em auditorias anteriores do PCI DSS, este status de descumprimento não ser conhecido, não ter sido involuntariamente divulgado ou não ter sido totalmente compreendido, o que pode fazer com que um serviço existente ou novo seja considerado fora de conformidade.

Se um serviço solicitado fazer com que o TPSP ou a entidade não esteja em conformidade com o PCI DSS ou se, durante o fornecimento do serviço, surgir uma situação que altere os atributos do serviço, pode ser apropriado determinar o impacto sobre a conformidade com o PCI DSS, tanto para a entidade quanto para o TPSP. Exemplos desses cenários podem incluir uma entidade que envia dados de autenticação confidenciais para seu TPSP para armazenamento, ou um TPSP que implementa uma mudança de infraestrutura que impacta os controles de segmentação entre os ambientes de suas entidades hospedadas. Recomenda-se que as seguintes ações sejam consideradas:

- Se um acordo não estiver atualmente em vigor entre a entidade e o TPSP — por exemplo, nova solicitação de serviço, novo relacionamento TPSP — recomenda-se que estes considerem realizar uma avaliação de risco adicional para determinar como proceder.
- Se existir um acordo entre a entidade e o TPSP, esta poderá considerar um exame do contrato ou acordo com o TPSP para determinar qual parte é responsável pela mitigação dos dados ou processos fora de conformidade.
 - Considere se o serviço ou processo fora de conformidade é essencial e o impacto de interrompê-lo assim que possível, até que uma solução possa ser desenvolvida.

- Para questões comerciais críticas, a entidade e o TPSP devem trabalhar juntos para determinar quem será responsável pelo custo e pela responsabilidade por corrigir o problema, se necessário. Discuta com um assessor jurídico para garantir que a entidade ou o TPSP e qualquer TPSP integrado usem disposições ou cláusulas de alteração de acordo/contrato adequadas para negociar um prazo justo e razoável para resolver a questão de não conformidade.
- Discuta com o TPSP e chegue a um acordo sobre a introdução de controles de compensação, assim que possível, que reduzam o risco de continuar com o processo ou troca de dados fora de conformidade, enquanto o trabalho continua em relação à resolução.
- Prepare um plano de resolução que possa ser fornecido à entidade ou ao TPSP em um formulário que possa ser usado como evidência (por exemplo, Planilha de controles de compensação) para fornecer um QSA, se uma análise de conformidade do PCI DSS for devida dentro do período de resolução.
- Garanta que os TPSPs integrados cumpram as obrigações acordadas com relação à resolução da não conformidade e mantenha os TPSPs informados sobre o progresso.

Anexo A: Pontos de discussão de alto nível para determinar a responsabilidade

Essas sugestões e pontos de discussão de alto nível podem ajudar a esclarecer como as responsabilidades dos requisitos do PCI DSS podem ser compartilhadas entre uma entidade e seu(s) TPSP(s). As entidades devem considerar definir essas responsabilidades em acordos por escrito com os TPSPs. A tabela neste Anexo também pode ajudar a preencher uma matriz de responsabilidades detalhada do PCI DSS (exemplo no **Anexo B**) e determinar quem será responsável por cada área de controle.

A tabela consiste nos seguintes campos:

- **Etapas para determinar a responsabilidade:** Áreas de controle de alto nível que podem abranger vários requisitos do PCI DSS e um ponto de partida para discussão entre a entidade e seu TPSP.
- **Pontos de discussão:** Pontos de discussão de alto nível para cada área de controle. Essas recomendações são para discussão entre a entidade e o TPSP, e visam a auxiliar na compreensão das áreas de controle e alocação das responsabilidades em cada uma delas.
- **Entidade ou terceiro:** Essas colunas podem ser usadas para monitorar a responsabilidade de cada área de controle pelos serviços prestados, quaisquer itens de discussão que precisem de acompanhamento ou se a área de controle é uma responsabilidade compartilhada.
- **Evidência a ser fornecida:** Esta coluna pode ser usada para documentar evidências a serem fornecidas, de mútuo acordo, pelo TPSP e pela entidade, para apoiar a validação da entidade em atender à área de controle.

Para obter o documento completo do PCI DSS e documentos relacionados, consulte o site do PCI SSC
https://www.pcisecuritystandards.org/security_standards/documents.php.

Observação: este Anexo destina-se apenas à orientação e é para uso opcional, a critério da entidade e/ou do TPSP; a conclusão deste Anexo não é um requisito. A alocação de responsabilidades entre uma entidade e seu(s) TPSP(s), em última análise, dependerá dos fatos e circunstâncias específicos, e dos serviços fornecidos. Embora os itens deste Anexo possam ser úteis para ajudar a alocar responsabilidades entre uma entidade e seus TPSPs, a lista de itens e pontos de discussão neste Anexo não é exaustiva. Cada empresa que busca contratar um TPSP deve determinar o que é relevante à luz das circunstâncias, do ambiente de pagamento da organização, da função proposta do TPSP e de outros fatores considerados importantes por meio de uma due diligence minuciosa.

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Componentes do sistema (por exemplo, firewalls, servidores, aplicativos, dispositivos)				
<p>Determinar os procedimentos para o projeto, preparação, implementação e manutenção contínua dos componentes do sistema.</p>	<ul style="list-style-type: none"> • Revisões de firewall • Criptografia de transmissões em redes públicas e sistemas de mensagens de usuário final • Atualizações e manutenção do sistema, incluindo <ul style="list-style-type: none"> ○ Ciclos de fornecimento de patches ○ Sistema operacional versus aplicativo ○ Virtual versus físico ○ Ferramentas e relatórios centralizados • Estratégias de isolamento (segmentação, detecção/prevenção de invasão) • Procedimentos de gestão de mudanças • Estratégias de implantação antivírus • Estratégia de detecção de alterações para arquivos críticos • Análise baseada em risco, incluindo resultados da avaliação de risco • Procedimentos de controle de acesso • Definição de funções <ul style="list-style-type: none"> ○ Processo de aprovação ○ Revisões de direitos ○ Procedimentos de revogação ○ Requisito de dois fatores ○ Requisitos de ID e senha ○ Limites de tempo de sessão e requisitos de login ○ Resposta a incidentes • Sincronização (Network Time Protocol) 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Determinar os procedimentos para testar a implementação e a manutenção contínua dos componentes do sistema.	<ul style="list-style-type: none"> • Testes funcionais • Verificações de vulnerabilidades de redes internas e externas <ul style="list-style-type: none"> - frequência • Testes de penetração (nível do aplicativo e da rede) • Detecção sem fio não autorizada • Detecção de pontos de acesso sem fio não autorizados. 			
Determinar a documentação necessária para atender a todos os requisitos aplicáveis do PCI DSS.	<ul style="list-style-type: none"> • Base de segurança de configuração do sistema • Diagramas de rede • Justificativa de portas, protocolos, serviços e daemons 			
Determinar os recursos e a documentação necessários para ajudar na produção de evidências e auxiliar na validação.	<ul style="list-style-type: none"> • Desenvolver a tabela RACI (responsável, aprovador, consultado, informado) para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação <ul style="list-style-type: none"> - Equipe de implementação - Administradores - Equipe de suporte - Gerentes - Responsáveis por testes de penetração - Segurança de TI - Equipe de gestão de mudanças - ASV - Equipe de resposta a incidentes 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Dados armazenados do titular do cartão				
Determinar períodos de retenção para armazenamento de dados do titular do cartão (CHD).	<ul style="list-style-type: none"> • Necessidades legais, regulatórias e comerciais. • Justificativa do armazenamento de CHD 			
Determinar os procedimentos para o descarte seguro de CHD.	<ul style="list-style-type: none"> • Trituração, redução a pasta de mídias físicas • Limpeza segura de mídia eletrônica 			
Determinar o procedimento para a verificação dos CHD que existem ou são transformados.	<ul style="list-style-type: none"> • Tecnologias de transformação (tokenização, criptografia, etc.) • Locais conhecidos onde os CHD são armazenados em todos os tipos de mídia • Aplicações, processos de negócios e locais físicos/lógicos onde os CHD mascarados são exibidos 			
Determinar os procedimentos para quaisquer tecnologias de transformação.	<ul style="list-style-type: none"> • Tipos de criptografia em uso • Procedimentos de destokenização, se disponíveis ou necessários • Procedimentos de gerenciamento de chaves, incluindo tabela RACI 			
Determinar os procedimentos para garantir que o armazenamento e o transporte dos dados do titular do cartão — incluindo a mídia física que contém dados do titular do cartão — sejam feitos com segurança.	<ul style="list-style-type: none"> • Backup de segurança de armazenamento de mídia • Revisar a frequência da segurança do local de armazenamento • Processo de distribuição de mídia • Classificação de mídia • Processo para todas as mídias enviadas fora da instalação • Frequência da enumeração do inventário de mídia 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
<p>Determinar os recursos e a documentação necessários para ajudar com:</p> <ul style="list-style-type: none"> • Produção de evidências • Validação 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação 			
Desenvolver e manter um código seguro				
<p>Determinar a metodologia de desenvolvimento de software de aplicativos e a segurança da informação no ciclo de vida do desenvolvimento de software.</p>	<ul style="list-style-type: none"> • Base dos processos de desenvolvimento de software (ou seja, padrões e/ou melhores práticas do setor) • Processos de revisão de código • Processos de treinamento em técnicas de codificação seguras (p. ex., OWASP) para desenvolvedores (baseados em melhores práticas e diretrizes do setor) 			
<p>Determinar os requisitos de RACI para ciclo de vida de desenvolvimento de software.</p>	<ul style="list-style-type: none"> • Separação dos deveres entre os ambientes de desenvolvimento/teste e de produção • Dados de produção (PANs ativos) usados para testes ou desenvolvimento • Resolução dos resultados/problemas de testes de vulnerabilidade e penetração • Gestão de alterações 			
<p>Determinar os recursos e a documentação necessários para ajudar com:</p> <ul style="list-style-type: none"> • Produção de evidências • Validação 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação <ul style="list-style-type: none"> – Recursos do desenvolvedor – Responsáveis por testes de aceitação do usuário (User-acceptance testing, UAT) – Responsáveis por testes de garantia de qualidade 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Acesso físico				
Determinar os procedimentos associados aos controles de segurança física para cada sala de computadores, data center e outras áreas físicas com sistemas no CDE.	<ul style="list-style-type: none"> • Viabilizar controles de entrada para limitar e monitorar o acesso físico aos sistemas no CDE 			
Determinar processos e procedimentos de atribuição de crachás para a equipe no local e para os visitantes.	<ul style="list-style-type: none"> • Visitantes • Equipe no local 			
Determinar os recursos e a documentação necessários para ajudar com: <ul style="list-style-type: none"> • Produção de evidências • Validação. 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação 			
Acesso ao CDE e/ou aos CHD				
Determinar os procedimentos associados à concessão, gerenciamento e monitoramento do acesso do usuário aos CHD ou ao CDE.	<ul style="list-style-type: none"> • Tipos de acesso a CHD/CDE <ul style="list-style-type: none"> ○ Interno ○ Externo • Concessão de credenciais • Revogação de credenciais • Funções e responsabilidades • Limitações de acesso 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Determinar os procedimentos associados à concessão, gerenciamento e monitoramento do acesso do fornecedor aos CHD ou ao CDE.	<ul style="list-style-type: none"> • Tipos de acesso a CHD/CDE <ul style="list-style-type: none"> ○ Interno ○ Externo • Concessão de credenciais • Revogação de credenciais • Funções e responsabilidades • Limitações de acesso 			
Determinar os recursos e a documentação necessários para ajudar com: <ul style="list-style-type: none"> • Produção de evidências • Validação 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução • Participação na avaliação <ul style="list-style-type: none"> ○ Concessão de acesso ○ Revogação de acesso ○ Monitoramento de acesso 			
Registro				
Estabelecer um processo para vincular todo o acesso aos componentes do sistema (principalmente o acesso realizado com privilégios administrativos como raiz) para cada usuário individual.	<ul style="list-style-type: none"> • Requisitos de registro central • Tipos de registros disponíveis-devem atender aos requisitos aplicáveis do PCI DSS • Proteção da integridade dos registros • Frequência da coleta de registros • Retenção de registros • Procedimentos de revisão e emissão de alertas <ul style="list-style-type: none"> ○ Coleta de registros ○ Análise de registros ○ Emissão de alertas • Procedimentos de assistência à investigação • Acesso ao sistema de registro 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
<p>Determinar os recursos e a documentação necessários para ajudar com:</p> <ul style="list-style-type: none"> • Produção de evidências • Validação 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Procedimentos operacionais diários ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação 			
<i>Manter uma política que aborde a segurança das informações para todas as equipes</i>				
Determinar quais políticas corporativas serão aplicadas para cada contratação.	<ul style="list-style-type: none"> • Qual política substituirá a outra, se necessário • Qual política será comunicada a todos os funcionários • Atende a todos os requisitos aplicáveis do PCI DSS 			
Determinar o processo para a avaliação de risco anual.	<ul style="list-style-type: none"> • Documentação da avaliação de riscos • Frequência da avaliação de riscos <ul style="list-style-type: none"> ○ Anualmente ○ Após alterações significativas 			
Determinar o plano para desenvolver um programa formal de conscientização da segurança para conscientizar todas as equipes sobre a importância da segurança dos dados do titular do cartão.	<ul style="list-style-type: none"> • Frequência de treinamento <ul style="list-style-type: none"> ○ Integração ○ Anualmente • Reconhecimento da equipe 			
Determinar os procedimentos para realizar verificações de antecedentes.	<ul style="list-style-type: none"> • Os procedimentos devem ser comparáveis • Considerações legais 			
Determinar o processo para a criação do programa de monitoramento do PCI.	<ul style="list-style-type: none"> • Atestado de conformidade • Termos da contratação 			

Etapas para determinar a responsabilidade	Pontos de discussão	Entidade	TPSP	Evidência a ser fornecida
Determinar o plano para desenvolver um plano de resposta a incidentes a ser implementado em caso de violação do sistema.	<ul style="list-style-type: none"> • Funções de resposta a incidentes, responsabilidades e estratégias de comunicação 			
Determinar recursos e documentação necessária para auxiliar com: <ul style="list-style-type: none"> • Produção de evidências • Validação 	<ul style="list-style-type: none"> • Desenvolver a tabela RACI para determinar os recursos necessários para ajudar com: <ul style="list-style-type: none"> ○ Políticas aplicáveis ○ Coleta de evidências ○ Assistência para resolução ○ Participação na avaliação 			

Anexo B: Exemplo da matriz de responsabilidades do PCI DSS

Uma matriz de responsabilidades do PCI DSS pode ajudar a esclarecer e confirmar como as responsabilidades para manter os requisitos do PCI DSS são compartilhadas entre a entidade e o TPSP. Os pontos de discussão de alto nível para determinar a responsabilidade no **Anexo A** podem ajudar na elaboração de uma matriz de responsabilidades detalhada do PCI DSS.

As considerações para cada requisito do PCI DSS incluem:

- O TPSP executa/gerencia/mantém o controle exigido?
- Como o controle é implementado e quais são os processos de suporte — por exemplo, o processo para atualizações de patches incluiria detalhes de testes, agendamento, aprovações, etc.?
- Como e quando o TPSP fornecerá garantia contínua e/ou evidência à entidade de que os controles são atendidos - por exemplo, relatórios periódicos, notificações em tempo real, resultados de testes, etc.?

Observação: este Anexo destina-se apenas para uso opcional, a critério da entidade e/ou do TPSP; a conclusão deste Anexo não é um requisito nem é necessário que uma entidade ou o TPSP conclua-o para atender ao Requisito 12.8.5¹⁵ do PCI DSS.

Requisito do PCI DSS	Responsabilidade			Cobertura/escopo específico da responsabilidade da entidade	Cobertura/escopo específico da responsabilidade do TPSP	Como e quando o TPSP fornecerá evidência de conformidade à entidade
	TPSP apenas	Entidade apenas	Compartilhada			
1.1 Defina e implemente os padrões de configuração do firewall e do roteador que incluam o seguinte:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.1 Um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.2 Diagrama atual da rede que identifica todas as conexões entre o ambiente dos dados do titular do cartão e outras redes, incluindo qualquer rede sem fio	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

¹⁵ Esta referência é ao PCI DSS v3.1 – Abril de 2015

Requisito do PCI DSS	Responsabilidade			Cobertura/ escopo específico da responsabilidade da entidade	Cobertura/ escopo específico da responsabilidade do TPSP	Como e quando o TPSP fornecerá evidência de conformidade à entidade
	TPSP apenas	Entidade apenas	Compartilhada			
1.1.3 Diagrama atual que mostra todos os fluxos de dados do titular do cartão em todos os sistemas e redes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.4 Requisitos para um firewall em cada conexão da internet e entre qualquer zona desmilitarizada (DMZ) e a zona de rede interna	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.5 Descrição de grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.6 Documentação e justificativa comercial para o uso de todos os serviços, protocolos e portas permitidas, incluindo a documentação dos recursos de segurança implementados para os protocolos considerados não seguros. <i>Exemplos de serviços, protocolos ou portas não seguros incluem, entre outros, FTP, Telnet, POP3, IMAP e SNMP v1 e v2.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.1.7 Requisito para analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.2 Elabore configurações de firewall e roteador que restrinjam as conexões entre redes não confiáveis e quaisquer componentes do sistema no ambiente de dados do titular do cartão. Observação: uma “rede não confiável” é qualquer rede que seja externa às redes que pertencem à entidade em análise e/ou que esteja além da capacidade da entidade de controlar ou gerenciar.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.1 Restrinja o tráfego de entrada e saída ao que é necessário ao ambiente de dados do titular do cartão e rejeite especificadamente todos os outros tráfegos.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1.2.2 Proteja e sincronize os arquivos de configuração do roteador.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
...e assim por diante.						

Agradecimento

O PCI SSC gostaria de agradecer a contribuição do Grupo de interesse especial em garantia de segurança de terceiros na preparação deste documento. Os membros incluem representantes das seguintes organizações:

2-sec Ltd.	Canadian Tire Financial Services
24 Solutions AB	Capita PLC
403 Labs, LLC	Chase Paymentech Solutions
7Safe	CIPHER
Accudata Systems	Citigroup Inc.
Accuvant, Inc.	City of Calgary
Acumera, Inc.	Civica UK Ltd
Agio, LLC	Coalfire Systems, Inc.
AJB Software Design	College Entrance Examination Board
Amazon.com	Comcast Cable Communications
American Express	Compass IT Compliance, LLC
American Lebanese Syrian Associated Charities Inc. (ALSAC)	Compliance3
Anitian Corporation	ComplyGuard Networks Inc.
ANXeBusiness Corp.	Comsec
Aon Service Corp.	Control Case
Assurant, Inc.	Control Gap
AT&T Consulting Solutions	ControlScan
atsec (Beijing) Information Technology Co., Ltd	Convergys Corporation
Australia Post	Credit Union Australia
Australian Payments Clearing Association (APCA)	Crowe Horwath LLP
Bank of America N.A.	CVS Caremark
Bank of New Zealand	Deli Management Inc.
Barclaycard	Dell, Inc.
Barnes & Noble College Booksellers Inc.	Deloitte & Touche LLP (USA)
Basefarm A/S	Digital Defense, Inc.
Baylor University	DSW Inc.
BB&T Corporation	ECS Security Ltd.
Bell Canada	EFM Consulting Inc.
Bill2Pay, an Intuition Systems Inc Company	Elavon Merchant Services
Bit9 Inc.	Espion LTD
Conselho de Curadores da University of Arkansas BP Products of North America	EVO Payments International
Bridge Point Communications	Experian Information Services
BrightLine CPAs & Associates, Inc.	Experis Finance US LLC
British Airways PLC	Fidelity Information Services (FIS)
BT Plc	FireHost
	Fiscal Systems, Inc.
	Fiserv Solutions Inc.
	Fishnet Security

Florida's Turnpike Enterprise	Nationwide Mutual Insurance Company
Foregenix	NBCUniversal
Foresight IT Consulting Pty Ltd.	NCC Group Plc
Fortrex	Nets Oy
G2 Web Services, LLC	Nettitude Ltd
G6 Hospitality LLC	Nexusguard Consulting Limited
Games Workshop Ltd	NIC Inc.
Gap Inc.	Nixu Ltd
GE Money	North Carolina State University
Gemserv Limited	NTT Data Intellilink Corporation
Global Payments Direct Inc.	NTT Security Ltd
Grant Thornton LLP	Paymetric Inc
GTT Communications Inc.	PayPal Inc.
GuidePoint Security, LLC	PayUSA
Heartland Payment Systems	Pen Test Partners
Henry Ford Health System	PetSmart, Inc.
Hitachi-Omron Terminal Solutions, Corp	Philips Electronics North America Corporation
HP Information Security UK Limited	Phillips Consulting Ltd
HyTrust Inc.	Post Office
IBM Corporation	PowerPay, LLC
Information Risk Management (IRM)	Praetorian Secure, LLC
Inline Technologies	PriceWaterhouseCoopers (PWC)
Integralis Ltd Europe	Privity Systems Inc.
Interac Association	Progressive Casualty Insurance Company
International Card Processing Services (ICPS) Ltd	Promocion y Operations SA de CV
Internet Security Auditors	Protiviti
IQ Information Quality	Rackspace
Kilrush Consultancy Ltd	Rapid7 LLC
KnowIT Secure AB	RBC Royal Bank
KPMG, LLP	RBS
La Maison Simons Inc.	Retalix Inc.
Levi Strauss and Co	RightScale Inc.
Limited Brands Inc.	Rockwell Collins
Lloyds Banking Group	RSM US, LLP
Lowe's Inc.	SecureConnect Inc.
M4 Products and Services	SecureWorks, Inc.
Mako Networks Ltd	Securisea, Inc.
Market America Inc	SecurityMetrics, Inc.
Marsh and McLennan Companies (MMC)	Security Risk Management
MegaPath Inc.	Sense of Security Pty Ltd
MegaplanIT, LLC	ServerChoice
Merchant Link, LLC	Sikich
Moneris Solutions Corp	LLP SISA
MoneyGram International	SITA

SIX Payment Services Ltd	UL Transaction Security
Solutionary, Inc.	University of North Carolina at Chapel Hill
Specialized Security Services, Inc.	University of Oklahoma
Sprint Nextel	U.S. Bancorp
SRC Security Research & Consulting GmbH	Vectra Corporation Ltd.
SSH Corporation	Vendor Safe Technologies
State Farm Mutual Automobile Insurance Company	VeriFone Inc.
StoreFinancial Services	Verizon/Cybertrust
Suncor Energy Inc.	VigiTrust
Symantec Corporation	Visa
SynerComm, Inc	Vodafone
SystemExperts Corporation	Vodat International Ltd
Sysnet Global Solutions	Voltage Security
Sysxnet Limited DBA Sysnet Global Solutions	Wal-Mart Stores Inc.
TD Bank NA	The Walt Disney Company
Telstra	Wayne Fueling Systems
Terra Verde LLC	Web.com
Tevora Business Solutions, Inc.	Westpac Banking Corporation
Time Warner Cable	WEX Inc.
TouchNet Information Systems, Inc.	WorldPay
Trustwave Holdings, Inc.	Wyndham Worldwide
TUI Travel Plc.	Xerox
TUV SUD Management Service GmbH	Xpient Solutions LLC

Sobre o PCI Security Standards Council

O PCI Security Standards Council é um fórum global aberto, que é responsável pelo desenvolvimento, gerenciamento, educação e conscientização dos Padrões de Segurança do PCI (PCI DSS) e outros padrões que aumentam a segurança de dados de pagamento. Criado em 2006 pelas bandeiras fundadoras de cartões de pagamento American Express, Discover Financial Services, JCB International, Mastercard e Visa Inc., o conselho tem mais de 650 empresas participantes representando comerciantes, bancos, processadores e fornecedores em todo o mundo. Para saber mais sobre como participar da proteção de dados de cartão de pagamento globalmente, acesse: pcisecuritystandards.org.