Security Standards Council®

Padrão:	Padrão de Segurança de Dados do PCI (PCI DSS)
Versão:	2.0
Data:	Novembro de 2012
Autor:	Risk Assessment Special Interest Group (SIG) PCI Security Standards Council (Conselho de Padrões de Segurança do PCI do Grupo de Interesse Especial [SIG] de Avaliação de Risco

Suplemento de Informações:

Diretrizes de avaliação de risco do PCI DSS

Índice

1 Introdução

1.1 Objetivo

O objetivo deste documento é fornecer orientação suplementar e recomendações para realizar uma avaliação de risco de acordo com o Requisito 12.1.2 do PCI DSS.

Uma avaliação de risco, conforme exigido no PCI DSS, é um processo formal usado pelas organizações para identificar ameaças e vulnerabilidades que poderiam afetar negativamente a segurança dos dados do portador do cartão.

Este documento não substitui nem estende quaisquer requisitos do PCI DSS; em vez disso, fornece orientação para que as organizações identifiquem, analisem e documentem os riscos que podem afetar seu ambiente de dados do portador do cartão (CDE).

1.2 Público-alvo

Esta orientação destina-se a qualquer organização que armazene, processe ou transmita dados do portador do cartão (CHD). Exemplos incluem comerciantes, prestadores de serviços, adquirentes (bancos comerciais) e emissores. O público-alvo inclui pequenas, médias ou grandes empresas.

2 Avaliações de risco e o PCI DSS

2.1 Definição de risco

O risco tem muitas interpretações e é frequentemente usado para descrever perigos ou ameaças a uma pessoa, ambiente ou negócio em particular. O que se segue é apenas uma definição:

> *Risco é uma função da probabilidade de uma determinada fonte de ameaça exercer uma vulnerabilidade potencial específica e o impacto resultante desse evento adverso na organização*[1]

Compreender o risco inclui o entendimento dos diferentes elementos e como eles se encaixam. Por exemplo, considerações de uma perspectiva empresarial podem incluir:

- Quais são os diferentes tipos de ameaças à organização?
- Quais são os ativos da organização que precisam de proteção contra as ameaças?
- Qual é o grau de vulnerabilidade de uma organização a diferentes ameaças?
- Qual é a probabilidade de uma ameaça ser realizada?
- Qual seria o impacto se uma ameaça fosse realizada?
- Como a organização pode reduzir a probabilidade de uma ameaça ser realizada ou reduzir o impacto se ela ocorrer?

2.2 Requisito do PCI DSS 12.1.2

Requisitos do PCI DSS	Procedimentos de teste
12.1 Definir, publicar, manter e disseminar uma política de segurança que realize o seguinte:	**12.1** Analise a política de segurança da informação e verifique se ela foi publicada e disseminada a todos os funcionários relevantes (incluindo fornecedores e parceiros comerciais).
12.1.1 Atende a todos os requisitos do PCI DSS.	**12.1.1** Verifique se a política atende a todos os requisitos do PCI DSS.
12.1.2 Inclui um processo anual que identifica ameaças e vulnerabilidades, e resulta em uma avaliação de risco formal. (Os exemplos de metodologias de avaliação de risco incluem, entre outros, OCTAVE, ISO 27005 e NIST SP 800-30.)	**12.1.2.a** Verifique se um processo anual de riscos, que identifica ameaças e vulnerabilidades, é documentado e resulta em uma avaliação de risco formal.
	12.1.2.b Analise a documentação da avaliação de risco para verificar se o processo de avaliação de risco é realizado ao menos anualmente.

Figura 1.0 – Requisito do PCI DSS 12.1.2

O Requisito do PCI DSS 12.1.2 exige que as organizações estabeleçam um processo anual que identifica ameaças e vulnerabilidades, e resulta em uma avaliação de risco formal.

[1] NIST SP800-30

Uma avaliação de riscos permite a uma organização identificar ameaças e as vulnerabilidades relacionadas que têm o potencial de causar um impacto negativo em seus negócios. Os recursos podem então ser alocados com eficácia para implementar controles que reduzem a probabilidade e/ou o impacto potencial das ameaças em questão.

Realizar avaliações de risco pelo menos anualmente permite que as organizações mantenham-se atualizadas com as mudanças de negócios e fornece um mecanismo para avaliar essas mudanças em relação ao cenário de ameaças em evolução, tendências emergentes e novas tecnologias. Exemplos de alterações incluem a introdução de uma nova linha de produtos ou oferta de serviço que é diferente dos produtos ou serviços existentes, introdução de um novo aplicativo de software no CDE, alteração de uma topologia de rede que afeta o CDE, etc.

2.3 Estratégia de gestão de risco

Como a avaliação de risco do PCI DSS leva em conta apenas um subconjunto dos riscos gerais da organização, as empresas devem maximizar os benefícios de uma avaliação de risco incorporando a avaliação do PCI DSS em seu programa geral de gerenciamento de risco em toda a organização.

O processo de avaliação de risco deve incluir pessoas, processos e tecnologias envolvidas no armazenamento, processamento ou transmissão de CHD, incluindo aqueles que podem não estar diretamente envolvidos no processamento dos CHD, mas ainda têm o potencial de impactar a segurança do CDE — por exemplo, a segurança do edifício de perímetro na instalação onde o CDE está localizado. Também deve-se levar em consideração os processos de negócios terceirizados e/ou gerenciados por prestadores de serviços ou comerciantes terceirizados.

Para garantir cobertura adequada, um programa de gestão de risco de toda a organização precisaria garantir que os riscos sejam considerados em todas as áreas da organização, que há uma estratégia coordenada para lidar com riscos identificados e que os esforços de atenuação de risco estejam alinhados em todos os processos de negócios.

2.4 Requisitos do PCI DSS

O PCI DSS fornece uma linha de base de controles técnicos e operacionais que trabalham juntos para fornecer uma abordagem de defesa detalhada para a proteção dos dados do titular do cartão. O PCI DSS compreende um conjunto mínimo de requisitos para proteger os dados do titular do cartão e pode ser aperfeiçoado por controles e práticas adicionais para amenizar os riscos ainda mais. As avaliações de risco fornecem informações valiosas para ajudar as organizações a determinar se controles adicionais são necessários para proteger seus dados confidenciais e outros ativos.

Observação: *O resultado de uma avaliação de risco não deve ser usado por organizações como meio de evitar ou ignorar os requisitos aplicáveis do PCI DSS (ou controles de compensação relacionados).*

Para obter conformidade com o PCI DSS, uma organização deve atender a todos os requisitos aplicáveis do PCI DSS.

2.5 Benefícios de conduzir uma avaliação de risco do PCI DSS

A realização de uma avaliação de risco do PCI DSS ajuda uma organização a identificar e compreender os possíveis riscos ao seu CDE. Ao compreender esses riscos, uma organização pode priorizar esforços de atenuação de riscos para abordar os riscos mais críticos primeiro. As organizações também podem implementar controles de redução de ameaças de forma mais eficaz, por exemplo, escolhendo uma tecnologia ou solução que melhor aborde riscos identificados.

As avaliações de risco podem ajudar a identificar a presença de dados do portador do cartão que não são fundamentais para as operações de negócios e que podem ser removidos do ambiente de uma organização, reduzindo o risco para o ambiente e potencialmente o escopo de seu CDE.

Além disso, as avaliações de risco podem identificar áreas que contêm dados que precisam de proteção e áreas que estão mais abertas e não precisam de acesso a dados confidenciais. As informações obtidas através de uma avaliação de risco podem ser usadas para determinar como segmentar ambientes para isolar redes sensíveis (CDE) de redes não sensíveis e, portanto, poupar investimentos desnecessários em controles de segurança onde não são necessários. O isolamento dessas redes menos sensíveis ajuda a definir o CDE e contribui para uma metodologia de escopo eficaz.

Realizar avaliações de risco em intervalos regulares fornece informações para a mudança de ambientes a uma organização e ajuda a identificar onde os controles de mitigação precisam ser ajustados ou adicionados antes que novas ameaças possam ser realizadas. Esta prática pode proporcionar a oportunidade de identificar se é possível garantir o investimento futuro em recursos.

Idealmente, um processo de avaliação de risco contínuo seria implementado para permitir a descoberta contínua de ameaças e vulnerabilidades emergentes que poderiam afetar negativamente o ambiente de dados do portador do cartão (CDE), permitindo que uma organização atenuasse tais ameaças e vulnerabilidades de forma proativa e oportuna.

2.6 Avaliação de risco e a abordagem priorizada

Para organizações que trabalham para sua validação de conformidade inicial do PCI DSS, a Abordagem Priorizada fornece um guia de atividades de conformidade com base no risco associado a armazenamento, processamento e/ou transmissão dos dados do portador do cartão. Ela ajuda as organizações a priorizar os esforços para alcançar a conformidade, estabelecer marcos e reduzir o risco de violações de CHD no início do processo de conformidade. Como parte do Marco 1, a organização precisa implementar um processo de avaliação de risco formalizado para identificar ameaças e vulnerabilidades que poderiam afetar negativamente a segurança dos dados do portador do cartão.

As organizações que trabalham em direção à conformidade podem achar que a avaliação inicial de risco requer tempo e recursos adicionais, pois pode ser a primeira vez que o ambiente foi analisado e avaliado a partir de uma perspectiva baseada em risco. Além disso, se um processo de avaliação de risco ainda não estiver estabelecido, as organizações precisarão definir e documentar sua metodologia de avaliação de risco, identificar indivíduos que precisarão estar envolvidos, atribuir funções e responsabilidades e alocar recursos.

Para organizações que mantêm a conformidade, é importante entender que a validação anual do PCI DSS é apenas um retrato da conformidade em dado momento, conforme observado no Relatório sobre Conformidade (ROC) ou Questionário de Autoavaliação (SAQ). Para garantir que a conformidade seja mantida, uma avaliação de risco pode ser realizada após quaisquer alterações significativas ao CDE, incluindo, entre outras, quaisquer mudanças em tecnologias, processos de negócios, pessoal e/ou relacionamentos de terceiros que possam afetar a segurança do CHD.

3 Metodologias de risco padrão do setor

3.1 Elementos comuns

Diversas metodologias aceitas pelo setor estão disponíveis para ajudar as organizações a desenvolverem seu processo de avaliação de risco. Exemplos dessas metodologias incluem:

- **A Organização Internacional de Padronização (ISO)** publicou uma ampla gama de padrões adequados à segurança da informação e à gestão de riscos. O documento mais relevante para compreender e fornecer orientação sobre a avaliação de risco é a *ISO 27005,* que é uma diretriz de gestão de risco. Esse documento abrange os processos padrão de gestão de risco de segurança da informação que são realizados englobando a avaliação de risco.

  A orientação fornecida na ISO 27005 é útil para conduzir avaliações de risco de segurança de informações formais.

- **O Instituto Nacional de Padrões e Tecnologia (NIST)** desenvolve padrões, métricas, testes e programas de validação para promover, medir e validar a segurança em sistemas e serviços de informação. A orientação geral sobre gestão de risco para sistemas de informação é abordada no Gerenciamento de risco de segurança da informação: organização, missão e visão do sistema informação (NIST SP 800-39), enquanto o NIST SP 800-30 (Revisão 1) concentra-se exclusivamente nas avaliações de risco. Grande parte do trabalho realizado pelo NIST se alinha ao trabalho realizado na Europa por organizações como ITSEC e, subsequentemente, Critérios comuns.
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation** ℠ **(OCTAVE®)** é um conjunto de ferramentas, técnicas e métodos para avaliação e planejamento estratégicos de segurança da informação baseados em risco. O método OCTAVE lista oito processos para uma avaliação de risco formal. Ele aproveita o conhecimento das pessoas sobre as práticas e processos relacionados à segurança de sua organização para capturar o estado atual de segurança dentro da organização. Riscos para os ativos mais críticos são usados para priorizar áreas de melhoria e definir a estratégia de segurança para a organização. Os recursos OCTAVE fornecem uma fonte útil de orientação.

Outras estruturas de risco, como a Análise de Fatores de Risco de Informação (FAIR) e o Padrão AS/NZS 4360 da Austrália/Nova Zelândia, podem ser usadas sozinhas ou para complementar avaliações realizadas usando metodologias tradicionais, como OCTAVE e aquelas publicadas pela ISO e NIST.

Todas as metodologias mencionadas acima têm metas comuns, embora a partir de perspectivas ligeiramente diferentes. Todas são adequadas para as avaliações de risco do PCI DSS. Cada metodologia de risco incorpora as seguintes atividades principais:

- Identificar ativos críticos e ameaças a esses ativos
- Identificar as vulnerabilidades, tanto organizacionais quanto tecnológicas, que poderiam potencialmente expor ativos a essas ameaças, resultando em risco para a organização
- Desenvolver uma estratégia de risco e planos de mitigação de riscos para abordar riscos identificados em apoio à missão e prioridades da organização

Muitas metodologias de avaliação de risco seguem etapas semelhantes; entretanto, as abordagens que elas realizam para identificar riscos e suas técnicas de medição diferem. A maioria das metodologias tem opções para ambas as abordagens *quantitativa* e *qualitativa* (discutidas posteriormente neste documento).

As organizações podem optar por incorporar uma metodologia de avaliação de risco formalizada, como aquelas abordadas acima, e adaptá-la à cultura e aos requisitos da organização.

4 Principais elementos de uma avaliação de risco

4.1 Desenvolver uma equipe de avaliação de risco

A equipe de avaliação de risco deve incluir a representação de todos os departamentos dentro da organização, incluindo aqueles envolvidos no processamento, armazenamento e transmissão de CHD. Esses departamentos podem incluir processos de negócios, tecnologia e departamentos de suporte, como recursos humanos, marketing, operações, tecnologia da informação, segurança da informação e administração de segurança.

Sempre que possível, recomenda-se que a avaliação de risco seja liderada por um indivíduo e/ou indivíduos que tenham conhecimento suficiente dos requisitos do PCI DSS e da metodologia de avaliação de risco sendo utilizada pela organização. O líder do processo de avaliação de risco é normalmente responsável por conduzir o processo de avaliação de risco dentro da organização e relatar os resultados à gerência. Organizações sem os recursos internos ou habilidades para realizar avaliações de risco podem considerar envolver recursos externos para auxiliar no processo de avaliação de risco.

4.2 Elaboração de uma metodologia de avaliação de risco

Ao desenvolver sua própria metodologia de avaliação de risco, as organizações podem considerar a adaptação de uma metodologia padrão do setor que seja mais apropriada para sua cultura e clima comercial em particular, para garantir que seus objetivos de risco específicos sejam cumpridos. A Figura 2.0 ilustra os componentes típicos da avaliação de risco.

Figura 2.0 – Componentes da avaliação de risco

4.2.1 Identificação do risco

Antes que uma organização possa avaliar seus riscos, ela deve compreender seus processos de negócios, ativos, ameaças e vulnerabilidades.

- **Estabelecimento de contexto –** A equipe de avaliação de risco precisa entender os parâmetros internos e externos ao definir o escopo da avaliação de risco e/ou ter acesso às pessoas na organização que possam fornecer essas informações — por exemplo, a hierarquia da organização, os processos de negócios, os fluxos de CHD e quaisquer componentes do sistema associados.
- **Identificação de ativos –** Geralmente, os ativos podem ser qualquer coisa de valor para uma organização. No contexto do PCI DSS, os ativos incluem as pessoas, os processos e as tecnologias envolvidas no processamento, armazenamento, transmissão e proteção da CHD. Cada ativo pode ser identificado para um proprietário do ativo que será, então, responsável por proteger adequadamente o ativo. Ele também pode receber um valor de ativo, baseado em sua importância e criticidade.

  Ao identificar ativos para uma avaliação de risco do PCI DSS, todos os canais de pagamento devem ser considerados, por exemplo, presencial, e-commerce, pedido de correio/pedido por telefone (MOTO), etc., porque os ativos identificados para cada canal de aceitação de pagamento podem apresentar diferentes níveis de risco.

  Para ajudar a classificar os ativos como relevantes para os negócios da organização, pode ser útil estruturar os ativos em grupos e subgrupos como aqueles mostrados na Figura 3.0:

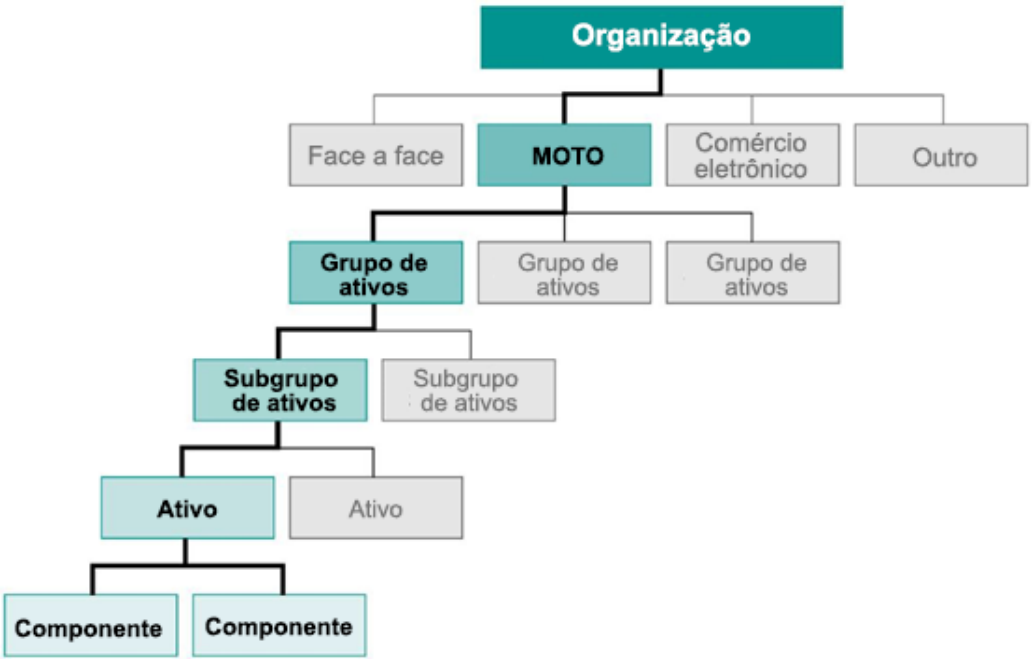

Figura 3.0 - Agrupamento de ativos

- **Identificação de ameaças –** As ameaças podem incluir as pessoas, os sistemas que usam e as condições que podem causar danos a uma organização. Conversar com a equipe em todas as áreas de uma organização ajudará o avaliador de riscos a entender onde eles veem o potencial de ameaças surgirem. Os funcionários em diversos níveis da organização terão perspectivas diferentes e podem fornecer informações que o avaliador de risco pode não ter considerado anteriormente.

  Além disso, incidentes de segurança que possam ter ocorrido, dentro da organização ou do setor, podem ser analisados para ajudar a organização a identificar possíveis ameaças. As ameaças são comumente medidas em termos da capacidade do "agente de ameaça" (qualquer coisa que tenha o potencial de perceber uma ameaça), a intenção do agente de ameaça, a relevância para a organização, a probabilidade de ocorrência de uma ameaça e o potencial de impactos adversos.

- **Identificação de vulnerabilidade –** Uma vulnerabilidade é um ponto fraco que pode ser explorado por uma ameaça e pode originar-se da tecnologia, da organização, do ambiente ou de um processo de negócios. Em uma avaliação de risco, todas as vulnerabilidades devem ser consideradas. Por exemplo, as vulnerabilidades podem ocorrer como resultado do projeto, desenvolvimento e/ou deficiências de implantação de sistemas ou software. Podem existir vulnerabilidades organizacionais e de processos de negócios devido a políticas e procedimentos inexistentes ou ineficazes. Vulnerabilidades podem ser identificadas a partir dos respectivos relatórios de avaliação, relatórios de teste de penetração e auditorias de segurança técnica, como revisões de regras de firewall, revisões de código seguro e revisões de configuração de banco de dados.

A Tabela 1.0 na página a seguir fornece apenas alguns exemplos de ameaças e vulnerabilidades, juntamente com o possível resultado e impacto para as operações de negócios de uma organização. Esta não é uma lista completa, pois uma organização encontrará muitas outras ameaças e vulnerabilidades que terão o potencial de afetar negativamente seus negócios.

Tabela 1.0 – Ameaças, vulnerabilidades, risco e impacto

Ameaças	Vulnerabilidades	Possível resultado/risco	Impacto potencial para o negócio
Hackers externos, indivíduos mal-intencionados, criminosos cibernéticos	▪ Falta de segurança de rede - por exemplo, firewalls configurados adequadamente, falta de detecção de invasão ▪ Política de senha fraca ▪ Transmissão de CHD desprotegidos ▪ Falta de conscientização de segurança para engenharia social, phishing ▪ Endurecimento insuficiente do sistema, proteção contra malware	▪ Invasão de rede ▪ Comprometimento das credenciais do usuário ▪ Comprometimento do sistema ▪ Introdução de código malicioso ▪ Tempo de inatividade do sistema ▪ Comprometimento de dados sensíveis	▪ Roubo de CHD e/ou SAD ▪ Impacto sobre a reputação ▪ Perda de negócios devido à menor confiança do cliente ▪ Interrupção dos processos de negócios ▪ Perda financeira — custo de recuperação, investigação forense, perda de receita, possíveis multas/penalidades
Indivíduos mal-intencionados internos, erros internos do usuário, erro humano	▪ Falta de controle de mudança eficaz ▪ Falta de conhecimento/treinamento do usuário ▪ Atribuição inadequada de permissões de acesso (por exemplo, não baseado na necessidade de saber ou menos privilégio) ▪ Falta de separação de tarefas ▪ Endurecimento insuficiente do sistema ▪ Fraca criptografia/práticas precárias de gerenciamento de chaves	▪ Introdução de código malicioso por meio de navegação na web/ e-mail ▪ Alterações não testadas do sistema ▪ Escalonamento de privilégios de contas de usuários ▪ Acesso não autorizado a dados confidenciais	

Ladrão/intruso com intenção de causar danos físicos ou roubar ativos	▪ Falta de segurança/monitor amento físico ▪ Manuseio não seguro dos terminais de pagamento ▪ Falta de detecção de violação ▪ Descarte de mídia de armazenamento sem excluir dados ▪ Falha em supervisionar adequadamente visitantes/fornece dores	▪ Roubo/substituição de terminais de pagamento ▪ Skimmers não detectados adicionados aos sistemas POS ▪ Acesso não intencional aos CHD ▪ Instalação de dispositivos invasores que levam ao comprometimento da rede

4.2.2 Criação de perfil de risco

O perfil de risco é a representação de todos os riscos para um ativo, juntamente com ameaças e vulnerabilidades e suas respectivas pontuações de risco. O perfil de risco permite que os proprietários de ativos avaliem os riscos e tomem medidas necessárias de atenuação destes.

O perfil de risco geralmente inclui o seguinte:

Tabela 2.0 – Características do perfil de risco

Categoria	Características
Ativos	▪ Tipo de ativo (ativo primário ou de suporte, informações ou processo de negócios, hardware ou software, etc.) ▪ Valor do ativo
Ameaça	▪ Propriedades da ameaça (interna ou externa, acidental ou deliberada, física ou de rede, etc.) ▪ Probabilidade/possibilidade de ameaça
Vulnerabilidades	▪ Descrição da vulnerabilidade ▪ Nível de vulnerabilidade
Risco	A pontuação do risco é uma função de: ▪ Valor do ativo ▪ Probabilidade de ameaça e ▪ Nível de vulnerabilidade

4.2.2.1 Controles existentes

Os controles existentes são aqueles que já estão presentes em uma organização para proteger contra ameaças e vulnerabilidades identificadas. A identificação dos controles existentes é necessária para determinar sua adequação. A eficácia dos controles existentes pode ser identificada através da revisão de políticas/procedimentos existentes, entrevista de pessoas, observação de processos e análise de relatórios de auditoria anteriores e registros de incidentes.

4.2.2.2 Avaliação de risco

A avaliação de risco permite que uma organização determine a importância dos riscos para priorizar os esforços de mitigação. Isso ajuda as organizações a obter o uso ideal dos recursos. As técnicas de medição de risco usadas durante o processo de avaliação podem ser quantitativas, qualitativas ou uma combinação de ambas:

a) **Avaliação quantitativa de risco –** Uma avaliação quantitativa de risco atribui valores numéricos aos elementos da avaliação de risco (geralmente em termos monetários). Isso é realizado incorporando-se dados históricos, avaliação financeira de ativos e tendências do setor.

   As avaliações de risco quantitativas podem ser consideradas mais objetivas do que as qualitativas de risco, pois são baseadas em informações estatísticas. No entanto, realizar uma avaliação puramente quantitativa é, frequentemente, difícil, já que pode não ser fácil determinar um valor monetário para alguns ativos, por exemplo, a “reputação” de uma organização.

b) **Avaliação qualitativa de risco –** As avaliações qualitativas de risco categorizam os parâmetros de risco de acordo com o nível de intensidade ou impacto para um ativo. A categorização dos parâmetros de risco é realizada através da avaliação dos componentes de risco usando julgamento especializado, experiência e consciência situacional. As escalas são tipicamente baseadas em um conjunto de valores escalonados — por exemplo, baixo, moderado e alto.

As Tabelas 2.1 e 2.2 são exemplos de algumas técnicas de medição comumente usadas. A Tabela 2.1 avalia o risco como um fator de impacto e probabilidade, enquanto a Tabela 2.2 representa o risco como um fator de valor do ativo, probabilidade de ameaça e facilidade de exploração.

Tabela 2.1 – Exemplo de uma matriz de cálculo de risco

		Consequência		
		Impacto insignificante	***Impacto moderado***	***Impacto importante***
Probabilidade	***Muito provável***	Risco médio	Alto risco	Alto risco
	Provável	Risco médio	Risco médio	Alto risco
	Possível	Baixo risco	Risco médio	Alto risco
	Improvável	Baixo risco	Baixo risco	Risco médio

Tabela 2.2 – Exemplo de uma matriz de cálculo de risco usando valor, ameaça e facilidade de exploração do ativo (ou nível de vulnerabilidade)

	Probabilidade de ameaça	**Baixa**			**Média**			**Alta**		
	Facilidade de exploração	**Baixa**	**Média**	**Alta**	**Baixa**	**Média**	**Alta**	**Baixa**	**Média**	**Alta**
Valor do ativo	***Baixa***	0	1	2	1	2	3	2	3	4
	Média	1	2	3	2	3	4	3	4	5
	Alta	2	3	4	3	4	5	4	5	6
	Muito alta	3	4	5	4	5	6	5	6	7
	Crítica	4	5	6	5	6	7	6	7	8

Baixo risco 0-2	Risco médio 3-5	Alto risco 6-8

Avaliações qualitativas de risco são mais subjetivas do que as quantitativas, mas podem resultar em melhor entendimento do negócio, bem como melhorar a comunicação entre os diferentes departamentos da empresa que contribuem para a avaliação de risco geral.

Em alguns casos, os números são atribuídos a cada valor para criar um equivalente numérico à escala. Por vezes, essa abordagem é chamada de medição "semiquantitativa". Esses métodos são usados quando não é possível usar os quantitativos ou quando há necessidade de reduzir a subjetividade em métodos qualitativos.

Muitas organizações realizam avaliações de risco usando uma combinação de métodos quantitativos e qualitativos.

4.2.3 Tratamento do risco

Assim que os riscos forem identificados e medidos, é importante definir estratégias de tratamento de risco. Como a eliminação de todo o risco é geralmente impraticável ou quase impossível, é importante implementar os controles mais adequados para diminuí-lo a um nível aceitável. As estratégias de tratamento de risco incluem:

- **Redução de risco** – Tomar as medidas de mitigação necessárias para reduzir o risco geral para um ativo. Muitas vezes, isso incluirá a escolha de contramedidas que reduzirão a probabilidade de ocorrência ou reduzirão a gravidade da perda ou alcançarão ambos os objetivos ao mesmo tempo. As contramedidas podem incluir controles técnicos ou operacionais ou alterações no ambiente físico. Por exemplo, o risco de vírus de computador pode ser reduzido pela aquisição e implementação de um software antivírus. Ao avaliar a força de um controle, deve-se considerar se os controles são preventivos ou de detecção. O nível de risco restante após os controles/contramedidas terem sido aplicados é frequentemente chamado de "risco residual". Uma organização pode optar por passar por um ciclo adicional de tratamento de risco para abordar isso
- **Compartilhamento/transferência de risco**[2] – A organização compartilha seu risco com terceiros através de seguros e/ou prestadores de serviços. O seguro é um mecanismo compensatório pós-evento, usado para reduzir a carga de perda se o evento ocorresse. A transferência é a troca de risco de uma parte para outra. Por exemplo, quando documentos impressos são movidos fora do local para armazenamento em um local de fornecedor de armazenamento seguro, a responsabilidade e os custos associados à proteção dos dados transferem-se para o prestador de serviços. O custo do armazenamento pode incluir a compensação (seguro) se os documentos forem danificados, perdidos ou roubados.
- **Prevenção de riscos –** A prática de eliminar o risco retirando-se ou não se envolvendo com a atividade que permite que o ele seja realizado. Por exemplo, uma organização decide descontinuar um processo empresarial para evitar uma situação que a exponha ao risco.
- **Aceitação de risco**[2] **–** Uma organização decide aceitar um risco em particular porque ele está dentro de seus parâmetros de tolerância e, portanto, ela concorda em arcar com o custo quando este ocorrer. A aceitação de risco é uma estratégia viável, na qual o custo do seguro contra o risco seria maior ao longo do tempo do que as perdas totais sustentadas. Todos os riscos que não forem evitados ou transferidos são aceitos por padrão.

2 ***Observação:*** *Uma avaliação de risco não pode resultar na aceitação, transferência ou compartilhamento de qualquer risco que resultará na não conformidade com quaisquer requisitos aplicáveis do PCI DSS.*

5 Riscos de terceiros

5.1 Riscos compartilhados com terceiros

As organizações podem terceirizar processos de negócios, obter serviços ou ter relações comerciais com comerciantes terceirizados, prestadores de serviços ou outras entidades que poderiam influenciar a segurança dos CHD. Realizar uma avaliação de risco é essencial para compreender o nível de risco que poderia ser introduzido na organização através da realização de negócios com comerciantes e/ou prestadores de serviços terceirizados. Os terceiros representam três áreas importantes a serem consideradas para a gestão de riscos: eles podem representar riscos, compartilhá-los ou gerenciá-los:

	Terceiros podem:	Por exemplo:
1	**Representar risco**	O desenvolvimento de um aplicativo que processa, armazena ou transmite CHD
2	**Gerenciar riscos**	Um processo de negócios terceirizado
3	**Compartilhar risco**	Um processo de negócios compartilhado

Figura 4.0 - Agrupamento de ativos

Uma única entidade de terceiros pode representar todas essas áreas ao mesmo tempo e afetar a postura de risco geral da organização. O primeiro passo para compreender os riscos representados por terceiros é conhecer o escopo do relacionamento comercial ou serviço fornecido por eles. Para identificar todos os terceiros aplicáveis, uma organização deve estudar seus fluxos de CHD e quaisquer processos de negócios envolvendo os CHD. Além disso, uma organização deve considerar terceiros envolvidos no desenvolvimento, operação ou manutenção de seu CDE (mesmo aqueles que não lidam diretamente com as informações do titular do cartão ainda podem ter um impacto indireto sobre o CDE da organização). Alguns exemplos de terceiros e/ou prestadores de serviços a serem considerados incluem:

- Desenvolvedores de aplicativos
- Provedores de datacenter
- Provedor de host na Web
- Provedores de armazenamento de dados
- Prestadores de serviços de destruição de dados/mídia/hardware
- Serviços gerenciados — por exemplo, operações de TI, segurança
- Equipes operacionais terceirizadas – por exemplo, call centers
- Subcontratados

Pode ser útil que as organizações compreendam os principais atributos de cada relacionamento com terceiros, incluindo, entre outros, se o terceiro está em conformidade com o PCI DSS (para casos em que o CDE é afetado) ou se o aplicativo de pagamento é compatível com PA-DSS (para desenvolvimento de aplicativos); o nível do prestador de serviços (frequentemente baseado no volume de transação); se os contratos legais apropriados estão em vigor entre terceiros e a organização em relação ao gerenciamento de CHD; e o número de pessoas ou sistemas no terceiro que têm acesso aos CHD.

Analisar os principais atributos de um terceiro, como aqueles listados acima, ajudará uma organização a estabelecer um nível de risco para cada terceiro envolvido no desenvolvimento, operação ou manutenção de seu CDE e ajudará a priorizar aqueles que parecem representar o mais alto nível de risco.

Além disso, deve ser observado que um terceiro pode ser dependente de outros terceiros para serviços essenciais relacionados ao PCI. Talvez não seja necessário ou apropriado estender a avaliação de risco ao segundo nível de terceiros, mas é apropriado saber que eles existem e podem causar um impacto.

5.2 Compartilhamento/transferência de riscos

Uma vez concluída a avaliação de risco, há várias opções de tratamento de risco possíveis. Elas foram discutidas anteriormente na Seção 4.2.3, Tratamento de risco, e cada um poderia ser aplicado a um terceiro.

A transferência de risco é uma das estratégias de tratamento de risco mais relevantes para terceiros, e uma organização pode gerenciar essa relação por meio de acordo por escrito, por meio de uma obrigação contratual que declara que o terceiro assume a responsabilidade pela segurança dos CHD que processa, armazena ou transmite em nome da organização. No entanto, o risco de reputação restante significa que é improvável que o risco total para uma organização seja realmente transferido.

Acordos por escrito podem ajudar a implementar processos para mitigar riscos de terceiros, mas é provável que seja necessária uma garantia adicional para avaliar se estes têm os controles e processos de segurança adequados em vigor.

Abordagens para o gerenciamento de riscos de terceiros podem incluir uma dependência de uma avaliação do PCI DSS do terceiro conduzido por um QSA e a conclusão de um ROC, ou onde o terceiro ateste a conformidade com o PCI DSS através de um questionário de autoavaliação. Alternativamente, a organização pode realizar uma avaliação de risco do comerciante terceirizado e/ou prestador de serviços com recursos internos e/ou trabalhar com o terceiro para determinar se este está gerenciando os riscos da empresa de forma satisfatória.

Recomenda-se que o acordo por escrito (conforme o Requisito 12.8.2 do PCI DSS) inclua o requisito para que o comerciante terceirizado e/ou prestador de serviços informe a organização no caso de ocorrer um incidente que afete adversamente os CHD da empresa. Além disso, ela pode desejar realizar uma avaliação de risco para determinar o impacto, etapas para retificação e prazos associados. A comunicação regular com o comerciante terceirizado e/ou prestador de serviços é recomendada para que os detalhes do incidente sejam conhecidos e o status possa ser relatado de volta às partes interessadas apropriadas, quando necessário.

Durante o processo de avaliação de risco, uma organização pode determinar que o negócio contínuo com o comerciante terceirizado e/ou prestador de serviços pode aumentar o risco geral da organização em relação aos CHD e pode tomar medidas apropriadas para reduzir seu risco residual a um nível aceitável. Essas medidas podem incluir a rescisão do relacionamento comercial com o terceiro. Como parte do processo anual de avaliação de riscos, quaisquer relações comerciais com comerciantes terceirizados e/ou prestadores de serviços devem ser reavaliadas.

6 Relatórios de resultados

Sugere-se que cada avaliação de riscos resulte em um respectivo relatório, detalhando os riscos identificados, incluindo aqueles que afetam o ambiente de dados do portador do cartão. O objetivo do relatório seria articular claramente os vários riscos que preocupam a organização e também podem explicar as ações tomadas por ela para remediar esses riscos. A tabela a seguir inclui tópicos sugeridos que um relatório pode conter.

Tabela 3.0 – Tópicos de relatório de avaliação de risco

Tópico	Explicação do conteúdo
Escopo da avaliação de risco	Um relatório de avaliação de risco deve descrever claramente a organização e os parâmetros internos e externos levados em consideração ao definir o escopo dessa avaliação. Isso pode incluir a finalidade da avaliação de risco, as tecnologias em vigor, processos comerciais, relacionamentos de terceiros, principais partes interessadas e quaisquer detalhes pertinentes adicionais. Para o objetivo do Requisito 12.1.2 do PCI DSS, o escopo também pode incluir uma visão geral do ambiente de dados do titular do cartão e as organizações envolvidas no suporte e operação do processamento dos dados do portador do cartão.
Inventário de ativos	Este processo envolve a confecção de uma lista abrangente de ativos que estão no escopo da avaliação de risco, por exemplo, software, hardware, infraestrutura de rede, comunicações e pessoal. Um inventário de ativos também pode incluir o valor de ativo, seu tipo, seu proprietário e a localização para cada ativo identificado.
Ameaças	Devem ser listadas as ameaças que podem prejudicar os ativos identificados. Essa lista também pode incluir uma descrição de cada ameaça para ajudar a entender as características das ameaças identificadas. A probabilidade de as ameaças ocorrerem será calculada com base na metodologia de avaliação de risco usada pela organização (expressa como uma probabilidade percentual ou uma classificação qualitativa, por exemplo, baixa, média ou alta).
Vulnerabilidades	O relatório de avaliação de risco também pode conter uma lista de vulnerabilidades, tanto tecnológicas quanto relacionadas à organização, que podem afetar os ativos desta. O tipo de ameaças que provavelmente aproveitará a vulnerabilidade também pode ser listado.
Avaliação de risco	O relatório deve descrever a técnica de medição de risco usada para priorizar os riscos identificados, por exemplo, medidas quantitativas ou qualitativas.

Tópico	Explicação do conteúdo
Tratamento do risco	O relatório de avaliação de risco deve documentar a lista de ações tomadas para cada um dos riscos identificados, juntamente com seu status de conclusão, por exemplo, redução de risco, transferência de risco, etc.
Histórico da versão	O relatório de avaliação de risco pode incluir a data, o autor e o aprovador do documento. A data de avaliação de risco pode ajudar a organização a monitorar a frequência de suas avaliações e a confirmar se elas são realizadas pelo menos anualmente, conforme exigido pelo Requisito 12.1.2 do PCI DSS.
Resumo executivo	Pode ser uma boa prática incluir um resumo executivo do relatório de avaliação de risco. Esse resumo pode detalhar a postura de risco da organização antes e depois de sua atenuação. O resumo também pode fornecer um painel adequado de riscos para gerenciamento com relação ao número de ativos, ameaças, vulnerabilidades e riscos.

7 Fatores críticos de sucesso

Identificação – A identificação correta dos ativos desempenha um papel importante no processo de avaliação de risco. Portanto, as organizações devem coletar informações de todas as partes interessadas (como recursos humanos, segurança da informação, departamentos comerciais, etc.) que estejam envolvidas no processamento, armazenamento e transmissão de CHD.

Para identificar adequadamente ameaças e vulnerabilidades, os avaliadores devem ter uma mente aberta e levar em conta as várias condições que poderiam afetar negativamente o CDE. Eventos históricos, relatórios de auditoria e incidentes de segurança dentro da organização ou setor também podem fornecer informações adicionais.

Abordagem proativa – O processo de avaliação de risco deve ser proativo em vez de reativo. Isso permitirá que a organização identifique, analise e documente proativamente seus riscos. Adotar uma abordagem proativa ajuda as organizações a evitar medidas corretivas dispendiosas. Portanto, há uma necessidade de monitoramento contínuo de riscos ao longo do ano.

Manter a simplicidade – O processo de avaliação de risco pode ser mantido de forma simples com o desenvolvimento de uma metodologia que melhor atenda às necessidades de uma organização. Metodologias padrão do setor publicadas podem ajudar neste processo.

As escalas de medição devem ser limitadas a um pequeno número de categorias. A inclusão de várias categorias frequentemente introduzirá uma complexidade desnecessária e reduzirá a probabilidade de que as partes interessadas de risco compreendam os resultados. Cada valor em uma escala de medição deve ser explicitamente definido. Sem definições claras, as partes interessadas muitas vezes formarão opiniões diferentes sobre os dados. Assim que as medições forem definidas, elas devem ser validadas pelos indivíduos que participaram do processo de avaliação de risco para garantir que os resultados sejam interpretados de forma consistente em toda a organização.

Treinamento – Também sugere-se que avaliadores de risco sejam treinados em processos formais de avaliação de risco para garantir que estejam melhor preparados para compreender as ameaças e vulnerabilidades que poderiam afetar negativamente a segurança dos dados do portador do cartão e, em última instância, a organização.

8 Agradecimentos

O PCI SSC gostaria de agradecer a contribuição do Grupo de Interesse Especial de Avaliação de Risco na preparação deste documento. Os membros incluem representantes das seguintes organizações:

ABC Financial Services	Liquid Networx
Accuvant Inc.	Market America, Inc.
Airlines Reporting Corporation	McGladrey LLP
A-lign Security and Compliance Services	Nationwide Building Society
AOL Inc.	PayPal Inc.
Assurant, Inc.	Progressive Casualty Insurance Company
Bank of America N.A.	Protegrity USA, Inc.
Bankalararası Kart Merkezi (BKM) A.Ş.	Retalix
Barclaycard	Royal Bank of Scotland Group
Bell Canada	SecureState LLC
BrightLine CPAs & Associates, Inc.	Security Risk Management Ltd
BT Counterpane	SecurityMetrics, Inc.
Capita Plc	Sense of Security Pty Ltd
CHS INC	SISA Information Security Inc.
CIPHER Security	Sprint Nextel
Citibank NA, Sucursal Uruguay	Store Financial Services, LLC
Coalfire, Inc.	Suncor Energy Inc.
Compass Group UK & Ireland Limited	Symantec Corp.
Crowe Horwath LLP	Tesco
D+H	Thales eSecurity Limited
Deloitte LLP - Reino Unido	The Co-operative Group
Deluxe Corporation	The Members Group
First Data Merchant Services	Tripwire, Inc.
Fiscal Systems, Inc.	Trustwave
Global Payments Inc.	TUI Travel PLC
HP Enterprise Security Services	VeriFone, Inc.
IQ Information Quality	Verizon Enterprise Solutions
Kilrush Consultancy Ltd.	Verizon Wireless
LBMC Security Services	Vodat International Ltd
Levi Strauss and Co.	Yum! Brands, Inc.

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 principais marcas de cartões de pagamento American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc., o Council tem mais de 600 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.