



Security
Standards Council®

Data: abril de 2018

Autor: Grupo de interesse especial em nuvem
PCI Security Standards Council

Suplemento de informações: Diretrizes de computação em nuvem do PCI SSC

Alterações no documento

Data	Versão	Descrição
Fevereiro de 2013	2.0	Publicação inicial das Diretrizes de computação em nuvem PCI DSS v2.0, produzidas pelo Cloud SIG de 2013.
Abril de 2018	3.0	<p>Diretrizes do PCI SSC atualizadas para computação em nuvem segura, produzidas pelo Cloud SIG de 2017. As alterações incluem:</p> <ul style="list-style-type: none">• Reestruturação do documento para melhor fluxo (por exemplo, consolidação das Seções 6.3 e 6.4, e mudança da Seção 6.5 para o Apêndice E).• Orientação atualizada sobre funções e responsabilidades, determinação do escopo dos ambientes de nuvem e desafios de conformidade do PCI DSS.• Orientação ampliada sobre resposta a incidentes e investigação forense.• Nova orientação sobre gestão de vulnerabilidades, bem como considerações técnicas adicionais de segurança sobre tópicos como redes definidas por software (Software Defined Networks, SDN), contêineres, computação em névoa e Internet das Coisas (Internet of Things, IoT).• Terminologia padronizada em todo o documento.• Referências atualizadas para recursos do PCI SSC e externos.• Pequenas atualizações gramaticais.

Índice

Alterações no documento	i
1 Introdução	1
1.1 Público-alvo	2
1.2 Terminologia	2
1.3 Resumo das recomendações.....	3
2 Visão geral da nuvem	5
2.1 Modelos de implantação em nuvem.....	5
2.2 Tipos de recursos de nuvem e categorias de serviço em nuvem	6
3 Relacionamentos com o provedor de nuvem/o cliente	8
3.1 Entendendo funções e responsabilidades	8
3.2 Funções e responsabilidades para diferentes modelos de implantação em nuvem.....	8
3.3 Responsabilidades para diferentes categorias de serviço em nuvem	9
3.4 Relacionamentos com provedores de serviços aninhados.....	11
4 Considerações do PCI DSS	13
4.1 Entendendo as responsabilidades do PCI DSS	13
4.2 Responsabilidades do PCI DSS para diferentes categorias de serviço em nuvem.....	13
4.3 Entendendo as responsabilidades de segurança como serviço (SECaaS)	16
4.4 Considerações sobre segmentação.....	16
4.4.1 Desafios de segmentação	17
4.4.2 Responsabilidades de segmentação.....	18
4.4.3 Tecnologias de segmentação	18
4.5 Considerações sobre determinação do escopo	19
4.5.1 Segurança dos sistemas do cliente de serviços em nuvem	21
4.5.2 Exemplos de determinação do escopo para diferentes modelos de implantação em nuvem	22
5 Desafios de conformidade do PCI DSS	26
5.1 O que significa quando um provedor afirma: "estou em conformidade com o PCI DSS"?	27
5.2 Verificação do escopo dos serviços e componentes validados do PCI DSS.....	27
5.3 Verificação dos controles do PCI DSS gerenciados pelo provedor de serviços em nuvem	28
6 Considerações sobre segurança	31
6.1 Governança, risco e conformidade.....	31
6.1.1 Gestão de risco	31
6.1.2 Devida diligência	32
6.1.3 Acordos de nível de serviço	32
6.1.4 Planos de continuidade de negócios e recuperação de desastres	33
6.1.5 Recursos humanos	33
6.2 Instalações e segurança física.....	33
6.3 Considerações sobre segurança de dados.....	34
6.3.1 Aquisição de dados	34
6.3.2 Armazenamento e persistência de dados	36
6.3.3 Uso de dados	36

6.3.4	Compartilhamento de dados	36
6.3.5	Descomissionamento e descarte	36
6.4	Resposta a incidentes e investigação forense	37
6.4.1	Resposta a incidentes	37
6.4.2	Investigação forense	38
6.4.3	Notificação de violação	39
6.5	Gestão de vulnerabilidades	39
6.5.1	Testes de vulnerabilidades dos aplicativos da Web	40
6.5.2	Varredura de vulnerabilidades da rede	41
6.5.3	Testes de penetração	42
6.5.4	Notificação de testes	43
Apêndice A: exemplo de responsabilidades do PCI DSS para diferentes categorias de serviço em nuvem		43
Apêndice B: inventário de amostras		50
Apêndice C: exemplo da matriz de gestão de responsabilidades do PCI DSS		52
Apêndice D: considerações sobre implementação do PCI DSS		54
Apêndice E: considerações sobre segurança técnica		60
E.1	Tecnologias de segurança em evolução	60
E.2	Multilocalização	60
E.3	Internet das Coisas e computação em névoa	61
E.4	Redes definidas por software	61
E.5	Sistemas de detecção de invasão (Intrusion Detection Systems, IDS)/sistemas de prevenção de invasão (Intrusion Prevention Systems, IPS)	63
E.6	Acesso e introspecção do hipervisor	64
E.7	Contêineres	66
E.8	Infraestrutura de desktop virtual na nuvem	68
E.9	Inventário e controle de recursos elásticos	71
E.10	Criptografia de dados e gerenciamento de chaves criptográficas	72
E.11	Dispositivos de criptografia segura na nuvem	73
E.12	Detecção de alterações para sistemas baseados em nuvem	74
E.13	Segurança de interfaces de software e APIs	75
E.14	Gerenciamento de identidade e acesso	75
E.15	Registros e trilhas de auditoria	76
Agradecimentos		78
Referências adicionais		78
Sobre o PCI Security Standards Council		79

1 Introdução

Computação em nuvem é uma forma de computação distribuída¹ que permite acesso a um conjunto expansível e elástico de recursos compartilháveis com provisionamento e administração sob demanda. Há vários fatores a serem considerados ao planejar o uso de serviços em nuvem e as organizações precisam entender claramente suas necessidades antes que possam determinar se e como elas serão atendidas por uma solução ou um provedor específico.

Essa orientação é destinada a organizações que usam ou estão pensando em usar, fornecer ou avaliar tecnologias de nuvem. Ela fornece diretrizes sobre o uso de tecnologias de nuvem e considerações referentes a como manter controles de segurança em ambientes de nuvem. Esse documento deve ser um ponto de partida para a discussão de provedores e clientes, e não pretende abordar configurações técnicas específicas ou situações em conformidade.

A orientação nesse documento é estruturada da seguinte forma:

- **Visão geral da nuvem** – Descreve os modelos de implantação em nuvem e modelos de serviço discutidos nesse documento.
- **Relacionamentos com o provedor de nuvem/o cliente** – Discute como as funções e responsabilidades podem diferir em modelos de serviços e de implantação em nuvem distintos.
- **Considerações do PCI DSS** – Fornece orientação e exemplos para ajudar a determinar as responsabilidades relacionadas a requisitos individuais do PCI DSS, e inclui considerações sobre segmentação e determinação do escopo.
- **Desafios de conformidade do PCI DSS** – Descreve alguns dos desafios associados à validação da conformidade do PCI DSS em um ambiente de nuvem.
- **Considerações sobre segurança** – Explora várias considerações sobre segurança comerciais e técnicas para o uso de tecnologias de nuvem.

Os apêndices a seguir fornecem orientação adicional:

- **Apêndice A: responsabilidades do PCI DSS em relação a diferentes modelos de serviço** – Apresenta considerações adicionais para ajudar a determinar as responsabilidades do PCI DSS em diferentes modelos de serviço em nuvem.
- **Apêndice B: inventário de amostras** – Apresenta um inventário do sistema de amostragem para ambientes de computação em nuvem.
- **Apêndice C: matriz de gestão de responsabilidades do PCI DSS** – Apresenta uma matriz de amostragem para documentar como as responsabilidades do PCI DSS são atribuídas entre o provedor e o cliente.
- **Apêndice D: considerações sobre implementação do PCI DSS** – Sugere um conjunto inicial de perguntas que poderão ajudar a determinar como os requisitos do PCI DSS podem ser atendidos em um ambiente de nuvem específico.
- **Apêndice E: considerações técnicas de segurança** – Fornece orientação sobre várias tecnologias baseadas em nuvem.

¹ Wayne Jansen and Timothy Grance, NIST Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, (Gaithersburg: National Institute of Standards and Technology, December 2011). <https://doi.org/10.6028/NIST.SP.800-144>.

As informações contidas nesse documento fornecem orientação suplementar e não substituem ou estendem os requisitos em qualquer padrão do PCI SSC, nem endossam o uso de quaisquer tecnologias, produtos ou serviços específicos. Para os fins deste documento, todas as menções feitas ao PCI DSS são referentes à versão 3.2; no entanto, os princípios e as práticas gerais aqui apresentados poderão ser aplicados além do contexto do PCI DSS.

1.1 Público-alvo

As informações nesse documento são destinadas a comerciantes, provedores de serviços, avaliadores e outras entidades que buscam orientação de como o uso da computação em nuvem poderá afetar a conformidade com o PCI DSS. Por exemplo:

- **Comerciantes** – Orientação de segurança e considerações do PCI DSS que são aplicáveis a ambientes de nuvem e poderão ser úteis para comerciantes que gerenciam sua própria infraestrutura de nuvem, bem como aqueles que buscam se envolver com terceiros. A orientação sobre como trabalhar com provedores terceirizados e sobre desafios de conformidade do PCI DSS também poderá ser útil.
- **Prestadores de serviços** – Orientação sobre segurança e considerações do PCI DSS que poderão fornecer informações úteis para auxiliar na compreensão dos provedores sobre os requisitos do PCI DSS e também poderão ajudar os provedores a entender melhor as necessidades dos clientes relacionadas ao PCI DS. A orientação sobre relacionamentos com provedores/clientes e desafios de conformidade do PCI DSS nesse documento também poderão ser úteis para os provedores.
- **Avaliadores** – Orientação sobre segurança e considerações do PCI DSS que poderão ajudar os avaliadores a entender do que precisam saber a respeito de um ambiente para poder determinar se um requisito do PCI DSS foi cumprido.

1.2 Terminologia

Além dos termos definidos no Glossário de termos, abreviações e acrônimos do PCI DSS, os seguintes termos são usados nesse documento:

- **Provedor de serviços em nuvem ("provedor")**: é a entidade que fornece o serviço em nuvem. Adquire e gerencia a infraestrutura necessária para fornecer os serviços, executa o software em nuvem que fornece os serviços e entrega os serviços de nuvem através do acesso à rede.²
- **Cliente de serviço em nuvem ("cliente")**: a entidade que assina um serviço prestado por um provedor. Poderá incluir comerciantes, provedores de serviços, processadores de pagamento e outras entidades que utilizam serviços em nuvem.
- **Usuário de serviço em nuvem**: pessoa ou entidade agindo em seu nome, associada a um cliente que usa serviços em nuvem. **Observação**: *exemplos de tais entidades incluem dispositivos e aplicativos*.³
- **Multilocação**: alocação de recursos físicos ou virtuais de modo que vários locatários de nuvem e seus cálculos e dados sejam isolados e estejam inacessíveis entre si.⁴
- **Locatário da nuvem**: um ou mais clientes que compartilham o acesso a um conjunto de recursos físicos e virtuais.

² Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger, and Dawn Leaf, Cloud Computing Reference Architecture, NIST Special Publication 500-92 (Gaithersburg: National Institute of Standards and Technology, September 2011). <https://dx.doi.org/10.6028/NIST.SP.500-292>.

³ Joint Technical Committee ISO/IEC JTC 1, Information technology – Cloud computing – Overview and vocabulary ISO/IEC 17788. <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

⁴ Ibid

1.3 Resumo das recomendações

Além das considerações comerciais e relacionadas a risco, a implementação de controles de segurança em um ambiente de nuvem requer conhecimento e competências técnicas especializadas. Portanto, é fundamental que antes de migrar as operações de cartões de pagamento para um ambiente de nuvem, o cliente envolva suas equipes técnica, jurídica, de devida diligência, de segurança da informação e de conformidade para trabalhar em conjunto com o objetivo de determinar suas necessidades e avaliar possíveis ofertas de serviço em nuvem em relação a essas necessidades.

Garantir que os serviços em nuvem sejam projetados, mantidos e usados com segurança é uma responsabilidade compartilhada entre o provedor e o cliente. É importante observar que todos os serviços em nuvem não são criados da mesma forma. Políticas e procedimentos claros devem ser acordados entre o cliente e o provedor para todos os requisitos de segurança. As responsabilidades de operação, gestão e notificação devem ser claramente definidas e compreendidas em relação a cada requisito, e reconhecidas, por escrito, em acordos contratuais.

Com relação a nuvens públicas ou de terceiros, os clientes devem considerar que, embora possam terceirizar a gestão operacional diária do ambiente de dados, eles são responsáveis pelos dados que colocam na nuvem. Os clientes são incentivados a "pesquisar" até encontrar um provedor que possa fornecer o nível de segurança e de garantia necessários.

As etapas a seguir devem ser cumpridas por qualquer organização que queira migrar para ou avaliar serviços em nuvem:

- ENTENDA seus requisitos de risco e de segurança primeiro.
- ESCOLHA um modelo de implantação que esteja alinhado com os requisitos de segurança e de risco, tanto os seus quanto os do seu setor.
- AVALIE diferentes opções de serviço.
- SAIBA o que você quer do seu provedor.
- COMPARE provedores e ofertas de serviços.
- FAÇA perguntas ao provedor e verifique as respostas; por exemplo:
 - No que cada serviço consiste exatamente e como o serviço é entregue?
 - O que o serviço oferece com relação à manutenção da segurança, à conformidade, à segmentação e à garantia do PCI DSS, e qual é a responsabilidade do cliente?
 - Como o provedor apresentará evidência contínua de que os controles de segurança continuam implementados e estão atualizados?
 - Com o que o provedor se comprometerá por escrito?
 - Há outras partes envolvidas na prestação de serviços, na segurança ou no suporte?
- DOCUMENTE tudo com seu provedor em acordos por escrito - por exemplo, acordos de nível de serviço (Service Level Agreements, SLAs)/contratos de termos de serviços etc.
- SOLICITE garantias por escrito de que os controles de segurança estarão em vigor e a verificação periódica (por exemplo, relatórios de conformidade) de que os controles continuam sendo mantidos.

- ANALISE o serviço e os acordos por escrito periodicamente para identificar se algo mudou.

Os provedores são incentivados a trabalhar com seus clientes para entender suas necessidades de segurança e de conformidade. Ambas as partes devem estar dispostas a manter a comunicação aberta e o monitoramento para evitar mal-entendidos ou lacunas nas responsabilidades de segurança.

Se os dados das contas forem armazenados, processados ou transmitidos em um ambiente de nuvem, o PCI DSS se aplicará a esse ambiente e a conformidade normalmente envolverá a validação do ambiente do provedor e o uso desse ambiente pelo cliente.

Os clientes têm a responsabilidade final pela segurança dos dados do titular do cartão.

Mesmo que um provedor possa afirmar que é compatível com o PCI DSS, o cliente deve confirmar que todos os serviços consumidos e os locais foram incluídos na validação de conformidade do PCI DSS do provedor e que os serviços sejam usados de forma compatível.

Além disso, a alocação da responsabilidade entre o cliente e o provedor quanto à gestão de controles de segurança não isenta um cliente da responsabilidade de garantir que os dados do seu titular do cartão (cardholder data, CHD) estejam devidamente protegidos de acordo com os requisitos aplicáveis do PCI DSS. Os clientes devem definir quais requisitos do PCI DSS são compartilhados entre o cliente, o provedor e quaisquer intermediários (por exemplo, um gateway de pagamento) e confirmar sua conformidade.

2 Visão geral da nuvem

A computação em nuvem fornece um modelo para permitir acesso à rede sob demanda a um conjunto compartilhado de recursos de computação (por exemplo: redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com mínimo esforço de gestão ou interação do provedor.⁵

A computação em nuvem pode ser usada para fornecer aos clientes acesso às tecnologias mais recentes sem um investimento caro em hardware e software. Graças às economias de escala associadas à entrega de serviços em nuvem, os provedores podem, com frequência, fornecer acesso a uma maior variedade de tecnologias e de recursos de segurança em comparação ao que o cliente poderia acessar de outra forma. Organizações que não dispõem de pessoal com competências técnicas aprofundadas também poderão desejar tirar proveito das competências e do conhecimento fornecidos pelo pessoal do provedor para gerenciar com segurança suas operações em nuvem.

Portanto, a computação em nuvem tem um potencial significativo para ajudar as organizações a reduzir a complexidade e os custos de TI, enquanto aumenta a agilidade. A computação em nuvem também é vista como um meio de acomodar requisitos comerciais visando à alta disponibilidade e redundância, inclusive continuidade dos negócios e recuperação de desastres.

2.1 Modelos de implantação em nuvem

Os modelos de implantação são definidos para distinguir entre diferentes modelos de propriedade e distribuição dos recursos usados para fornecer serviços em nuvem. Os ambientes de nuvem poderão ser implantados em uma infraestrutura privada, infraestrutura pública ou uma combinação de ambas. Os modelos de implantação mais comuns incluem:⁶

- **Nuvem pública:** modelo de implantação em nuvem em que os serviços em nuvem estão potencialmente disponíveis para qualquer cliente e os recursos são controlados pelo provedor. Uma nuvem pública poderá ser possuída, gerenciada e operada por uma organização comercial, acadêmica ou governamental ou alguma combinação delas. Ela está presente nas dependências do provedor. A disponibilidade real para clientes específicos poderá estar sujeita a regulamentações jurisdicionais. As nuvens públicas têm limites muito amplos, em que o acesso do cliente a serviços de nuvem pública tem poucas restrições, se houver.
- **Nuvem privada:** modelo de implantação em nuvem em que os serviços em nuvem são usados exclusivamente por um único cliente e os recursos são controlados por esse cliente. Uma nuvem privada poderá ser possuída, gerenciada e operada pela própria organização ou por um terceiro e pode estar presente dentro ou fora das dependências. As nuvens privadas buscam estabelecer um limite estritamente controlado em torno da nuvem privada com base na limitação dos clientes para uma única organização.
- **Nuvem comunitária:** modelo de implantação em nuvem em que os serviços em nuvem apoiam e são compartilhados exclusivamente por um grupo específico de clientes que têm requisitos compartilhados e um relacionamento entre si, e em que os recursos são controlados por pelo menos um membro desse grupo. Uma nuvem comunitária poderá ser possuída, gerenciada e operada por uma ou mais das organizações na comunidade, por um terceiro ou por alguma combinação deles, e poderá estar presente dentro ou fora das dependências. As nuvens comunitárias limitam a participação a um grupo de clientes que têm um conjunto compartilhado de objetivos, em contrapartida à abertura das nuvens públicas, enquanto as nuvens comunitárias têm participação mais ampla do que as nuvens privadas.

⁵ Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing Special Publication 800-145, NIST Special Publication 800-145 (Gaithersburg: National Institute of Standards and Technology, December 2011). <https://doi.org/10.6028/NIST.SP.800-145>.

⁶ Joint Technical Committee ISO/IEC JTC 1.

Essas preocupações compartilhadas incluem, entre outras, missão, requisitos de segurança da informação, políticas e considerações sobre conformidade.

- **Nuvem híbrida** – A infraestrutura em nuvem é uma composição de duas ou mais nuvens (privadas, comunitárias ou públicas) que permanecem entidades exclusivas, mas estão ligadas pela tecnologia para permitir a portabilidade. As nuvens híbridas frequentemente são usadas para fins de redundância ou de balanceamento de carga—por exemplo, os aplicativos dentro de uma nuvem privada podem ser configurados para utilizar recursos de computação de uma nuvem pública, conforme necessário, durante períodos de pico de capacidade (às vezes chamados "cloud-bursting").

2.2 Tipos de recursos de nuvem e categorias de serviço em nuvem

As categorias de serviço em nuvem ("**<Algo>-como-serviço**") identificam diferentes opções de controle para o cliente e o provedor. Por exemplo, os clientes SaaS simplesmente usam os aplicativos e serviços fornecidos pelo provedor, enquanto os clientes IaaS mantêm o controle dos seus próprios ambientes hospedados na infraestrutura subjacente do provedor. O National Institute of Standards and Technology (NIST) define três tipos de categorias de serviços em nuvem.⁷

Software como serviço (Software as a Service, SaaS) – Capacidade para os clientes utilizarem os aplicativos do provedor executados em uma infraestrutura de nuvem. Os aplicativos são acessíveis a partir de vários dispositivos através de uma interface thin client, como um navegador da Web ou de uma interface do programa.

Plataforma como serviço (Platform as a Service, PaaS) – Capacidade para os clientes implantarem seus aplicativos (criados ou adquiridos) na infraestrutura da nuvem, usando linguagens de programação, bibliotecas, serviços e ferramentas compatíveis com o provedor.

Infraestrutura como serviço (Infrastructure as a Service, IaaS) – Capacidade para os clientes utilizarem o processamento, o armazenamento, as redes e outros recursos de computação fundamentais do provedor para implantar e executar sistemas operacionais, aplicativos e outros softwares em uma infraestrutura em nuvem.

Existem outros padrões e estruturas que definem diferentes vocabulários e arquiteturas de referência (por exemplo, ISO/IEC 17788:2014), que, em grande parte, são comparáveis aos termos e às categorias definidas pelo NIST. Visando à consistência, este documento de orientação usa a terminologia do NIST (ou seja, SaaS, PaaS e IaaS) para descrever as categorias de serviço dos serviços do provedor.

As principais diferenças entre as categorias de serviço em nuvem dizem respeito ao modo como o controle é compartilhado entre o cliente e o provedor, o que, por sua vez, afeta o nível de responsabilidade de ambas as partes. Deve-se observar que, além de uma situação de nuvem privada autogerida, o cliente raramente tem qualquer controle sobre hardware, e é o grau em que os componentes virtuais, aplicativos e softwares são gerenciados pelas diferentes partes que distinguem as categorias de serviço em nuvem. Via de regra, o SaaS fornece aos clientes a menor quantidade de controle, enquanto o IaaS oferece o maior controle para o cliente. A Figura 1 mostra como o controle normalmente é compartilhado entre o provedor e o cliente em diferentes categorias de serviço.

⁷ Wayne Jansen and Timothy Grance, NIST Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, (Gaithersburg: National Institute of Standards and Technology, December 2011). <https://doi.org/10.6028/NIST.SP.800-144>.

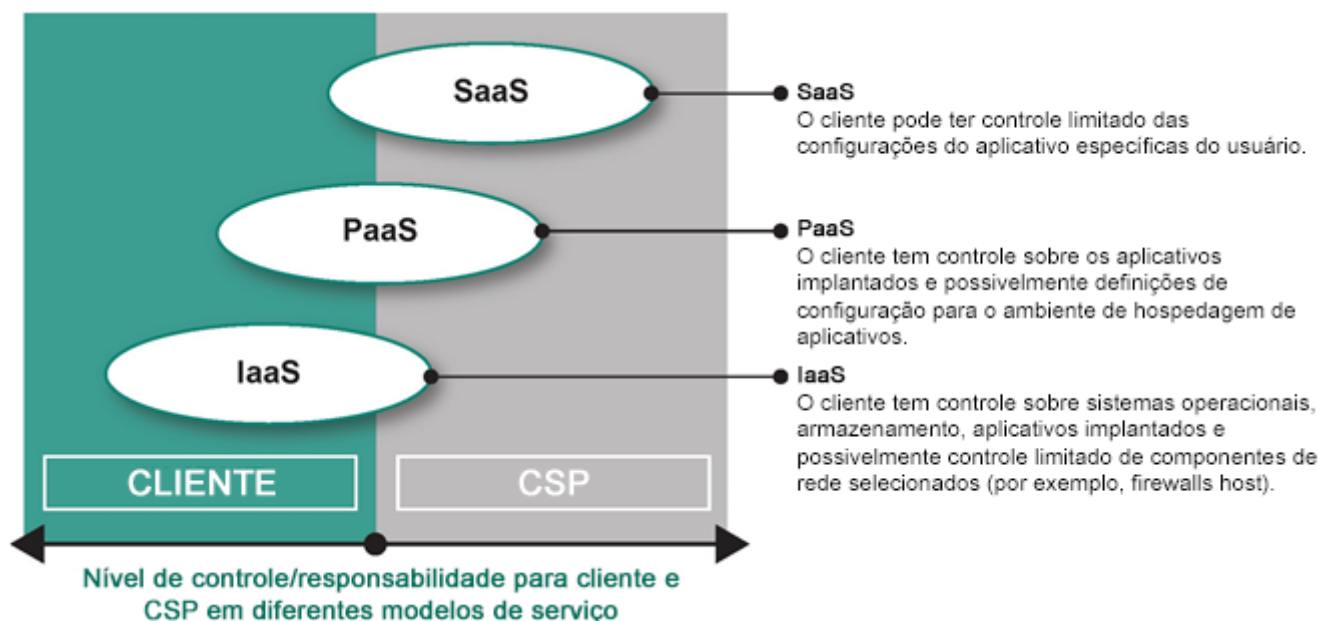


Figura 1: nível de controle/responsabilidade para o cliente e o provedor em diferentes categorias de serviço

O nível de responsabilidade de segurança nas categorias de serviços em nuvem geralmente migra para o cliente conforme o cliente passa de uma categoria SaaS (menor responsabilidade do cliente) para uma categoria IaaS (maior responsabilidade do cliente). O maior nível de responsabilidade para o provedor manter controles de segurança e operacionais está presente na categoria de serviço SaaS.

Embora os clientes possam ser atraídos pelas categorias SaaS e PaaS devido à economia de recursos e redução da responsabilidade pela administração do ambiente de nuvem, eles devem estar cientes de que essas categorias também correspondem a uma maior perda de controle do ambiente que abriga seus dados confidenciais.

Acordos contratuais e devida diligência contínua se tornam especialmente críticos onde o controle é terceirizado para garantir que as medidas de segurança necessárias estejam sendo atendidas e mantidas pelo provedor ao longo da vigência do acordo.

É importante observar que essas descrições para modelos de implantação em nuvem e categorias de serviços em nuvem, embora agora padronizadas e amplamente aceitas pelo setor, poderão não ser universalmente seguidas pelos provedores ou refletir os ambientes de nuvem reais. Por exemplo, um provedor pode estar vendendo um serviço de "nuvem privada" que não atenda à intenção de "privado" conforme descrito acima. Da mesma forma, os detalhes de o que está e não está incluído em um serviço específico provavelmente variam entre os provedores, mesmo se identificarem seus serviços pelo mesmo termo (IaaS, PaaS ou SaaS).

Espera-se que, à medida que o setor e os requisitos do cliente evoluam conforme as ofertas de nuvem amadurecerem, haverá categorias de serviço em nuvem adicionais além das listadas acima. No entanto, esse documento de orientação se concentra nas três principais categorias de serviço em nuvem: SaaS, PaaS e IaaS.

3 Relacionamentos com o provedor de nuvem/o cliente

3.1 Entendendo funções e responsabilidades

As linhas de prestação de contas e responsabilidade serão diferentes para cada categoria de serviço em nuvem e modelo de implantação, e serão regidas pelos acordos contratuais assinados. Os clientes não devem fazer suposições sobre qualquer serviço; políticas e procedimentos claros devem ser acordados entre o cliente e o provedor para todos os requisitos de segurança, e responsabilidades claras relacionadas à operação, à gestão e à notificação precisam ser definidas para cada requisito.

O PCI Security Standards Council publicou o Suplemento de informações *Garantia de segurança de terceiros*, que fornece mais orientações sobre a implementação do programa de garantia de terceiros.⁸

3.2 Funções e responsabilidades para diferentes modelos de implantação em nuvem

A entidade que desempenha o a função de provedor irá variar de acordo com o tipo do modelo de implantação. Por exemplo, a função do provedor poderá ser atribuída inteiramente a um terceiro externo (como em uma nuvem pública) ou a função poderá ser desempenhada por um departamento interno ou função comercial (como em uma nuvem privada no local). Da mesma forma, a função do provedor poderá ser atribuída a mais de uma entidade em uma situação de nuvem comunitária ou híbrida.

Para entender como as responsabilidades são atribuídas em um modelo de implantação específico, considere o seguinte:

- **Nuvem pública** – O provedor é um terceiro organizacionalmente separado de seus clientes. A nuvem é implantada no ambiente de um provedor e a responsabilidade é delineada de acordo com a categoria de serviço em nuvem específica, conforme definido pelo provedor.
- **Nuvem privada** – Quando uma nuvem privada é gerenciada no local, a função do provedor poderá ser desempenhada dentro do quadro funcional do cliente. Por exemplo, o departamento de TI poderia assumir a função de provedor com vários departamentos operacionais como seus clientes. Nessa situação, o cliente mantém o controle total do seu ambiente e a responsabilidade por sua segurança e conformidade.

Nuvens privadas exclusivas também poderão ser provisionadas fora das dependências por um provedor terceirizado. Nesse caso, o delineamento da responsabilidade também dependerá da categoria de serviço em nuvem específica, conforme descrito na Seção 3.3, “Responsabilidades para diferentes categorias de serviço em nuvem”.

- **Nuvem híbrida** – A função de provedor poderá ser atribuída a entidades internas e de terceiros para diferentes elementos da infraestrutura em nuvem geral. A responsabilidade será atribuída com base na combinação de modelos de implantação e das categorias de serviço em nuvem implementadas.
- **Nuvem comunitária** – O provedor poderia ser um dos clientes dentro da comunidade ou um terceiro separado. O delineamento da responsabilidade segue a categoria de serviço em nuvem específica implementada. A responsabilidade pela implementação, operação e gestão de controles de segurança será compartilhada de forma diferente dentro de cada uma das categorias de serviço em nuvem e precisa ser claramente compreendida pelo cliente e pelo provedor. O cliente também precisa entender o nível de supervisão ou visibilidade que terá sobre as funções de segurança que estão fora do seu controle. Se essas responsabilidades de segurança não forem adequadamente atribuídas,

⁸ Garantia de segurança de terceiros e responsabilidades compartilhadas Grupos de interesse especial e PCI Security Standards Council, *Garantia de segurança de terceiros* (PCI SSC, março de 2016), https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.

comunicadas e compreendidas, configurações inseguras ou vulnerabilidades poderiam passar despercebidas e não ser abordadas, resultando em possível exploração e perda de dados ou outro comprometimento.

3.3 Responsabilidades para diferentes categorias de serviço em nuvem

Em todos os modelos de implantação e, especialmente, em ambientes de nuvem pública, é importante que todas as partes compreendam os elementos específicos da categoria de serviço em nuvem usada e seus riscos associados. Qualquer modelo de implantação em nuvem que não seja totalmente autogerido é, por natureza, um modelo de responsabilidade compartilhada em que uma parte da responsabilidade do serviço em nuvem recai sob o âmbito do provedor (consulte a Seção 3.4, “Relacionamentos com provedores de serviços aninhados” para obter mais informações) e outra parte da responsabilidade também cai sobre cada cliente. O nível de responsabilidade que recai sobre o provedor ou o cliente é determinado pela categoria de serviço em nuvem sendo utilizada, por exemplo, IaaS, PaaS ou SaaS. O delineamento claro das responsabilidades deve ser estabelecido como pré-requisito para qualquer implementação de serviço em nuvem para fornecer uma referência para a operação em nuvem.

A Tabela 1 ilustra como o controle das diferentes camadas técnicas é frequentemente compartilhado em diferentes categorias de serviço em nuvem. Para fins de ilustração, diferentes camadas da pilha de nuvem são descritas da seguinte forma:

Camada	Descrição
Interface do programa de aplicativo (Application Program Interface, API) ou interface gráfica do usuário (Graphical User Interface, GUI)	A interface pela qual os usuários de serviço em nuvem interagem com o aplicativo. A API mais comum atual é RESTful HTTP ou HTTPS. A GUI mais comum atual é um site baseado em HTTP ou HTTPS.
Aplicativo	O aplicativo real sendo usado por um ou mais usuários do serviço em nuvem
Pilha de soluções ou pilha de tecnologia	É a linguagem de programação usada para desenvolver e implantar aplicativos. Os exemplos são .NET, Python, Ruby, Perl etc.
Sistemas operacionais (Operating Systems, OS)	Em um ambiente virtualizado, o sistema operacional é executado dentro de cada VM. Ou, se não houver nenhum hipervisor subjacente, o sistema operacional será executado diretamente no hardware de armazenamento.
Máquina virtual (Virtual Machine, VM)⁹	Um contêiner virtual executado em um hipervisor em um host. Um conjunto de tecnologias de isolamento de sistema que fornecem vários graus de isolamento de segurança com o kernel de OS da máquina de hospedagem
Contêineres	Técnica de virtualização que permite a execução de múltiplas instâncias de espaço de usuário isolado enquanto compartilha o mesmo kernel de OS subjacente
Infraestrutura de rede virtual	Para comunicações dentro e entre máquinas virtuais
Hipervisor	Quando a virtualização é usada para gerenciar recursos, o hipervisor é responsável pela alocação de recursos para cada máquina virtual. Ele também poderá ser aproveitado para implementar a segurança.

⁹ Os provedores frequentemente distinguirão entre a virtualização Paravirtual (PV) e Hardware Virtual Machine (HVM). O cliente deve estar familiarizado com a diferença e considerar seu impacto sobre o PCI DSS ou preocupações com o isolamento do processo.

Camada	Descrição
Processamento e memória	O hardware físico que fornece tempo e memória física da CPU
Armazenamento de dados	O hardware físico usado para o armazenamento de arquivos
Rede	Pode ser uma rede física ou virtual. É responsável por transportar comunicações entre sistemas e possivelmente a internet.
Instalação física	O edifício físico real onde os sistemas de nuvem estão localizados

O Apêndice B ilustra um inventário de amostragem para sistemas de computação em nuvem para fins de orientação sobre como os provedores e clientes podem documentar as diferentes camadas do ambiente de nuvem.

Tabela 1: exemplo de como o controle pode ser atribuído entre o provedor e o cliente em diferentes categorias de serviços em nuvem

	Cliente
	Provedor
	Compartilhado

Responsabilidade	Modelos de serviço		
	IaaS	PaaS	SaaS
Governança, risco e conformidade (Governance, Risk and Compliance, GRC) de segurança	Cliente	Cliente	Cliente
Segurança de dados	Cliente	Cliente	Cliente
Segurança de aplicativos	Cliente	Cliente	Compartilhado
Segurança da plataforma	Cliente	Compartilhado	Provedor
Segurança da infraestrutura	Compartilhado	Provedor	Provedor
Segurança física	Provedor	Provedor	Provedor

Observação: esta tabela fornece um exemplo de como as responsabilidades podem ser atribuídas de acordo com descrições comuns das diferentes categorias de serviço em nuvem. No entanto, é importante observar que as camadas de tecnologia e suas linhas de responsabilidade correspondentes poderão ser diferentes para cada provedor, mesmo se usarem a mesma terminologia para descrever seus serviços, e as ofertas de serviços individuais poderão ou não se alinhar com as atribuições de responsabilidade indicadas acima.

Alguns provedores oferecem várias opções para seus serviços, por exemplo, um provedor poderá ter uma oferta IaaS que inclui um hipervisor controlado pelo cliente e uma oferta separada de IaaS sem acesso do cliente ao hipervisor. É fundamental que os clientes e os provedores documentem e compreendam claramente onde estão os limites em suas relações específicas, em vez de supor que qualquer modelo de responsabilidade determinado se aplique a eles.

Mesmo quando um cliente não tem controle sobre uma camada específica, ele ainda poderá ter alguma responsabilidade pelas configurações ou definições que o provedor mantém em seu nome. Por exemplo, um cliente talvez tenha de definir regras de firewall e revisar conjuntos de regras de firewall para aqueles firewalls aplicáveis à proteção do seu ambiente, mesmo que o provedor realmente configure e gerencie os firewalls. Da mesma forma, os clientes poderão ser responsáveis pela aprovação e revisão das permissões de acesso do usuário aos seus recursos de dados, enquanto o provedor configura o acesso de acordo com as necessidades do cliente.

A alocação da responsabilidade quanto à gestão de controles de segurança não isenta um cliente da responsabilidade de garantir que os dados do seu titular do cartão estejam devidamente protegidos.

3.4 Relacionamentos com provedores de serviços aninhados

Relacionamentos com provedores de serviços aninhados são comuns em situações de nuvem, pois, às vezes, os provedores dependem de departamentos internos ou de outras empresas terceirizadas para entregar aspectos de seus serviços. Por exemplo, alguns provedores usam provedores de armazenamento terceirizados como parte de sua oferta de serviços em nuvem e alguns podem firmar parcerias com outros provedores para fins de redundância ou de tolerância a falha como parte de sua estratégia de entrega em nuvem.

Um exemplo de relacionamentos com provedores de serviços aninhados está ilustrado na Figura 2 abaixo:

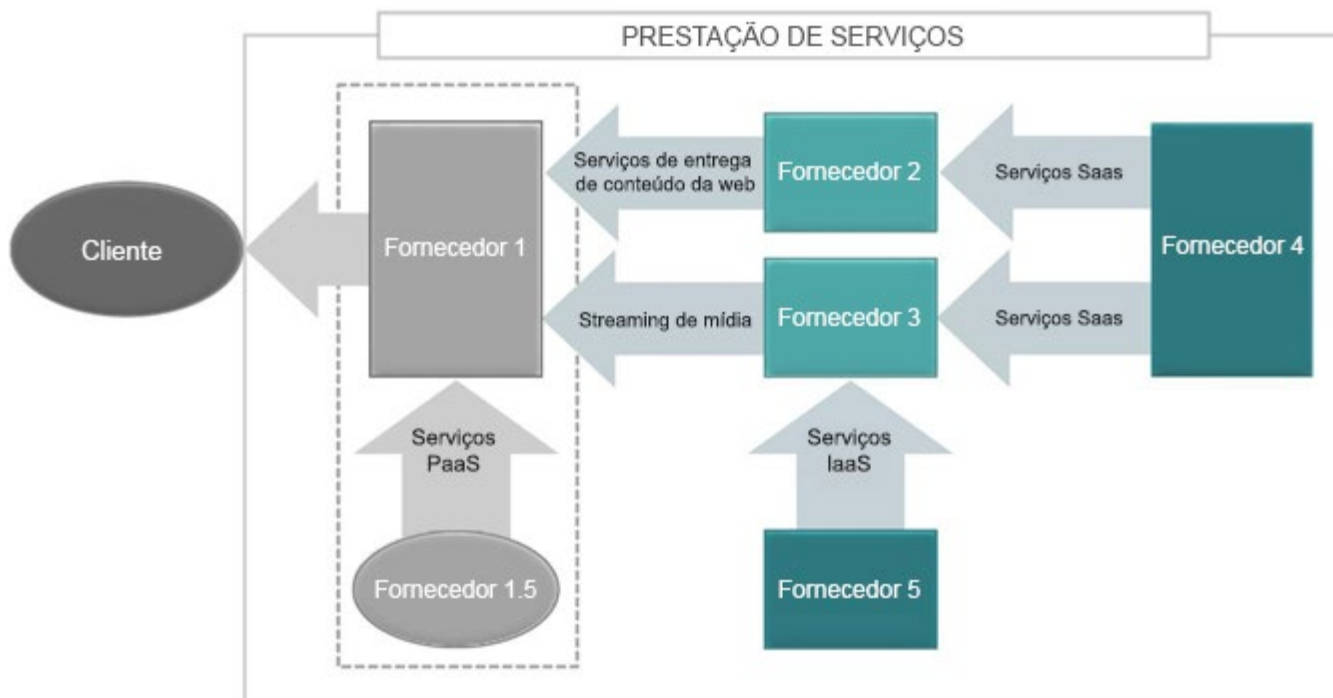


Figura 2: exemplo de relacionamentos com provedores de serviços aninhados

- O provedor 1 conta com o provedor 2 para serviços de entrega de conteúdo na Web e com o provedor 3 para streaming de mídia, bem como com o provedor 1.5 (nuvem interna/privada) para PaaS.
- O provedor 4 fornece serviço SaaS aos provedores 2 e 3.
- O provedor 5 fornece serviço IaaS ao provedor 3.

Pode haver várias camadas ou níveis de dependência do provedor, o que pode afetar a segurança do ambiente do titular do cartão. Identificar todos os relacionamentos com terceiros que o provedor tem em vigor é importante para compreender as possíveis ramificações para o ambiente de um cliente. A existência de vários relacionamentos aninhados, por exemplo, onde há uma cadeia de provedores e outros provedores necessários para a entrega de um serviço em nuvem, também adicionará complexidade ao processo de avaliação do PCI DSS do provedor e do cliente.

Quando o cliente tiver um relacionamento contratual direto com todos os provedores aninhados, o cliente precisará entender o impacto que cada provedor tem sobre seu CDE e como as responsabilidades do PCI DSS são gerenciadas para cada serviço. Quando o cliente não tiver relacionamentos contratuais com todos os provedores aninhados, o cliente confiaria no provedor principal (ou seja, o provedor com o qual o cliente tem um relacionamento direto e que, por sua vez, gerencia relacionamentos com os provedores aninhados) para gerenciar os relacionamentos e as responsabilidades do PCI DSS para todos os provedores envolvidos na entrega do serviço. Em ambos os casos, pode ser útil comunicar esses relacionamentos ao cliente (considere usar a Matriz de responsabilidades do PCI DSS opcional) para que ele possa compreender as considerações sobre conformidade do PCI DSS para todos os componentes do serviço.

Além disso, os clientes também poderão aproveitar essas informações de relacionamento dos provedores aninhados para devida diligência pré-contratação (Requisito 12.8), bem como os seguintes processos:

- Definição de perfil e gestão de riscos
- Continuidade dos negócios e planejamento de recuperação de desastres
- Monitoramento de ameaças
- Gestão da cadeia de suprimentos

4 Considerações do PCI DSS

4.1 Entendendo as responsabilidades do PCI DSS

As responsabilidades delineadas entre o cliente e o provedor quanto à gestão dos controles do PCI DSS são influenciadas por diversas variáveis, incluindo, entre outras:

- O objetivo para o qual o cliente está usando o serviço em nuvem
- O escopo dos requisitos do PCI DSS que o cliente está terceirizando para o provedor
- Os serviços e componentes do sistema que o provedor validou dentro de suas próprias operações
- A opção de serviço que o cliente selecionou para contratar o provedor (por exemplo, IaaS, PaaS ou SaaS)
- O escopo de quaisquer serviços adicionais que o provedor esteja fornecendo para gerenciar proativamente a conformidade do cliente (por exemplo, serviços de segurança gerenciados adicionais)

O cliente precisa entender claramente o escopo de responsabilidade que o provedor está aceitando para cada requisito do PCI DSS e quais serviços e componentes do sistema são validados para cada requisito. Por exemplo, os Requisitos 6.1 e 6.2 do PCI DSS atendem às necessidades de identificar e de classificar vulnerabilidades de acordo com o risco, e de implantar patches ausentes em tempo hábil. Se não houver uma definição apropriada, um cliente poderia supor que o provedor está gerenciando esse processo em relação a todo o ambiente de nuvem, enquanto o provedor poderia estar gerenciando vulnerabilidades apenas para sua infraestrutura subjacente e presumindo que o cliente está gerenciando vulnerabilidades relacionadas a sistemas operacionais e aplicativos.

4.2 Responsabilidades do PCI DSS para diferentes categorias de serviço em nuvem

Via de regra, quanto mais aspectos das operações de um cliente são gerenciados pelo provedor, maior é a responsabilidade do provedor para manter os controles do PCI DSS. No entanto, terceirizar a manutenção dos controles não é a mesma que terceirizar a responsabilidade em relação aos dados em geral. Os clientes não devem fazer suposições sobre qualquer serviço e devem divulgar com clareza em contratos, memorandos de entendimento ou SLAs exatamente qual parte é responsável por proteger quais componentes e processos do sistema.

A Tabela 2 fornece um exemplo de como as responsabilidades referentes aos requisitos do PCI DSS poderão ser compartilhadas entre clientes e provedores em algumas das várias categorias de serviços em nuvem. Obviamente, haverá exceções e variações em cada serviço individual e esta tabela é fornecida como uma diretriz para os clientes e provedores com o objetivo de ajudar a planejar discussões e negociações.

As responsabilidades foram identificadas da seguinte forma:

- **Cliente** – Geralmente, cada cliente terá a responsabilidade de manter e verificar o requisito.
- **Provedor** – Geralmente, o provedor manterá e verificará o requisito para seus clientes.

- **Compartilhada** – Geralmente, a responsabilidade é compartilhada entre o cliente e o provedor. Isso poderá ser devido ao requisito que se aplica aos elementos presentes no ambiente do cliente e ao ambiente gerenciado pelo provedor, ou porque ambas as partes precisam estar envolvidas na gestão de um controle específico.

O Apêndice A inclui considerações adicionais para determinar como as responsabilidades do PCI DSS poderão ser atribuídas para cada categoria de serviço em nuvem.

O Apêndice C ilustra uma amostra da Matriz de responsabilidades do PCI DSS, como uma orientação sobre como os provedores e clientes podem documentar as atribuições de responsabilidade do PCI DSS.

O conceito de responsabilidade compartilhada ou conjunta pode ser particularmente complicado para se lidar. Embora alguns serviços e funções serão relativamente simples em relação ao escopo e estabelecerão limites, muitos serviços e funções irão se sobrepor se não forem claramente demarcados no início do relacionamento de serviço.

Onde o provedor mantém a responsabilidade pelos controles do PCI DSS, o cliente ainda é responsável por monitorar a conformidade contínua do provedor para todos os requisitos aplicáveis. Os provedores devem ser capazes de fornecer aos seus clientes a garantia contínua de que os requisitos estão sendo cumpridos, e onde o provedor está gerenciando requisitos em nome do cliente, deverá haver mecanismos em vigor para fornecer ao cliente os registros aplicáveis para demonstrar que os controles de segurança necessários estão em vigor – por exemplo, registros de auditoria mostrando todos os acessos aos dados do cliente.

Os clientes ainda são obrigados a validar sua conformidade de acordo com os programas das marcas de pagamento.

Tabela 2: exemplo de compartilhamento de responsabilidade do PCI DSS entre clientes e provedores

	Cliente
	Provedor
	Compartilhada

Requisito do PCI DSS	Exemplo de atribuição de responsabilidade para a gestão de Controles		
	IaaS	PaaS	SaaS
1: Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão.	Compartilhada	Compartilhada	Provedor
2: Não usar padrões disponibilizados pelo provedor para senhas do sistema e outros parâmetros de segurança.	Compartilhada	Compartilhada	Provedor
3: Proteger os dados armazenados do titular do cartão.	Compartilhada	Compartilhada	Provedor
4: Codificar a transmissão dos dados do titular do cartão em redes abertas e públicas.	Cliente	Compartilhada	Provedor
5: Proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus.	Cliente	Compartilhada	Provedor
6: Desenvolver e manter sistemas e aplicativos seguros.	Compartilhada	Compartilhada	Compartilhada
7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de divulgação dos negócios.	Compartilhada	Compartilhada	Compartilhada
8: Identificar e autenticar o acesso aos componentes do sistema.	Compartilhada	Compartilhada	Compartilhada
9: Restringir o acesso físico aos dados do titular do cartão.	Provedor	Provedor	Provedor
10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão.	Compartilhada	Compartilhada	Provedor
11: Testar regularmente os sistemas e processos de segurança.	Compartilhada	Compartilhada	Provedor
12: Manter uma política que aborde a segurança das informações para todas as equipes.	Compartilhada	Compartilhada	Compartilhada
Apêndice A1 do PCI DSS: requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada	Provedor	Provedor	Provedor

Observação: Os exemplos de responsabilidades ilustrados nessa tabela não incluem consideração sobre quaisquer atividades ou operações realizadas fora de uma oferta hipotética de serviço em nuvem. Essa tabela fornece um exemplo de como as responsabilidades do PCI DSS podem ser atribuídas de acordo com descrições comuns das diferentes categorias de serviço em nuvem. No entanto, cada provedor define, em última análise, seu próprio serviço e ofertas de serviços específicas poderão ou não ser consistentes com as ilustradas acima. Os clientes e provedores devem documentar claramente suas responsabilidades conforme aplicável aos seus acordos específicos.

4.3 Entendendo as responsabilidades de segurança como serviço (SECaaS)

A segurança como serviço, ou SECaaS, às vezes é usada para descrever a entrega de serviços de segurança usando uma categoria de serviço em nuvem baseada em SaaS. Embora as soluções de SECaaS não estejam diretamente envolvidas no armazenamento, no processamento ou na transmissão de CHD, elas ainda podem integrar a segurança do CDE e, portanto, é importante entender por quais controles do PCI DSS o provedor de SECaaS é responsável. Como exemplo, uma solução antimalware baseada em SaaS poderá ser usada para atualizar assinaturas antimalware nos sistemas do cliente através de um modelo de entrega em nuvem. Nesse exemplo, a oferta de SECaaS está fornecendo um controle do PCI DSS para o ambiente do cliente, e a funcionalidade de SECaaS precisará ser revisada para verificar se está atendendo aos requisitos aplicáveis.

O SECaaS pode variar em complexidade de um modelo de assinatura de aplicativo baseado em nuvem relativamente simples à terceirização complexa de todas as funções de segurança, como um Centro de operações de segurança (Security Operation Center, SOC) ou um Centro de operações de rede (Network Operation Center, NOC) usando modelos de entrega em nuvem. O número de requisitos aplicáveis do PCI DSS que se enquadram sob a responsabilidade do provedor de SECaaS aumentará em relação à complexidade do serviço sendo fornecido. Os comerciantes que usam SECaaS devem incluir provedores de serviços de SECaaS na lista dos provedores de serviços do PCI e garantir a conformidade com, no mínimo, os Requisitos 12.8.1 a 12.8.5 do PCI DSS para cada provedor de serviços de SECaaS usado.

4.4 Considerações sobre segmentação

Fora de um ambiente de nuvem, os ambientes de entidades individuais normalmente seriam física, organizacional e administrativamente separados uns dos outros. Os clientes que utilizam uma nuvem pública ou compartilhada de outra forma devem garantir que seus ambientes sejam adequadamente isolados dos demais locatários da nuvem.

Além de impor a separação entre os ambientes do cliente, a segmentação também poderá ser desejada no ambiente de um cliente para isolar seus componentes de CDE de componentes não relacionados a CDE a fim de reduzir seu próprio escopo do PCI DSS.

A segmentação em uma infraestrutura de computação em nuvem deve fornecer um nível de isolamento equivalente ao possível através da separação física da rede. Mecanismos para garantir o isolamento adequado poderão ser necessários na rede, no sistema operacional e nas camadas de aplicativos; e, mais importante, deve haver um isolamento garantido dos dados armazenados (consulte a Seção 4.4.3, “Tecnologias de segmentação”, para obter mais informações). Ambientes de nuvem de locatários devem ser isolados entre si que possam ser considerados entidades gerenciadas separadamente sem conectividade entre eles. Os provedores devem testar a segmentação (Requisito 11.3.4) entre todas as entidades dentro do seu controle pelo menos semestralmente e demonstrar os resultados.

Quaisquer sistemas ou componentes compartilhados pelos clientes em ambientes multilocatários, inclusive o hipervisor e os sistemas subjacentes, não devem fornecer um caminho de acesso entre ambientes. Qualquer infraestrutura compartilhada usada para hospedar um ambiente de cliente dentro do escopo estaria dentro do escopo para a avaliação do PCI DSS do cliente.

Em um ambiente híbrido, a responsabilidade por confirmar a segmentação é compartilhada pelo provedor e pelo cliente. Confirmar que a segmentação está efetivamente isolando o CDE apoia o cliente ao simplificar e minimizar o CDE (em vez de, por exemplo, toda a sua rede local ser incluída em seu CDE). Além disso, é responsabilidade do cliente garantir que o link ou a conexão ao provedor, bem como quaisquer dispositivos

(por exemplo, roteador físico no local, gateway de nuvem ou redes de trânsito de emparelhamento etc.) usados para facilitar a conexão, sejam protegidos e gerenciados.

Existe um ambiente de nuvem segmentado quando o provedor impõe o isolamento entre clientes em ambientes multilocatários. Exemplos de como a segmentação poderá ser fornecida em ambientes de nuvem compartilhados incluem, entre outros:

- Modelo de provedor de serviço de aplicativos (Application Service Provider, ASP) tradicional, em que servidores fisicamente separados são fornecidos para o ambiente de dados do titular do cartão (cardholder data environment, CDE) de cada cliente
- Servidores virtualizados que são individualmente dedicados a um cliente específico, inclusive qualquer armazenamento virtualizado, como Redes de área de armazenamento (Storage Area Networks, SANs), Armazenamento conectado à rede (Network Attached Storage, NAS) ou servidores de banco de dados virtuais
- Ambientes em que os clientes executam seus aplicativos em partições lógicas separadas usando imagens separadas do sistema de gestão de banco de dados e não compartilham armazenamento em disco ou outros recursos

O avaliador do PCI DSS deve validar a eficácia da segmentação para garantir que ele forneça isolamento adequado. Se a segmentação adequada for fornecida entre os locatários da nuvem (em um ambiente multilocatário), apenas o ambiente do cliente e o ambiente e os processos gerenciados pelo provedor estariam dentro do escopo para a avaliação do PCI DSS de um cliente. Entretanto, se a segmentação adequada não estiver em vigor ou não puder ser verificada, todo o ambiente de nuvem multilocatário estaria dentro do escopo para todas as avaliações dos clientes hospedados naquele ambiente. Exemplos de ambientes de nuvem não segmentados incluem, entre outros:

- Ambientes em que as organizações usam a mesma imagem de aplicativo no mesmo servidor e só são separadas pelo sistema de controle de acesso do sistema operacional ou do aplicativo
- Ambientes em que as organizações usam imagens diferentes de um aplicativo no mesmo servidor e só são separadas pelo sistema de controle de acesso do sistema operacional ou do aplicativo
- Ambientes em que os dados das organizações são armazenados na mesma instância do armazenamento de dados do sistema de gestão do banco de dados

Sem segmentação adequada, todos os locatários da nuvem da infraestrutura compartilhada, bem como o provedor, precisariam ser verificados como estando em conformidade com o PCI DSS para que qualquer cliente tivesse a garantia da conformidade do ambiente. Isso provavelmente tornará a validação de conformidade inalcançável para o provedor ou para qualquer um dos seus clientes.

4.4.1 Desafios de segmentação

A segmentação em ambientes hospedados tradicionais pode ser aplicada através de servidores físicos separados e medidas de segurança impostas usando métodos conhecidos. A diferença em um ambiente de nuvem é que há camadas compartilhadas comuns (como hipervisores e camadas de infraestrutura virtual) que podem apresentar um único ponto de entrada (ou ataque) para todos os sistemas acima ou abaixo dessas camadas compartilhadas. A segurança aplicada a essas camadas é, portanto, essencial não apenas para a segurança dos ambientes individuais que elas apoiam, mas também para garantir que a segmentação seja imposta entre diferentes ambientes de nuvem de locatários.

Uma vez que qualquer camada da arquitetura de nuvem seja compartilhada por ambientes CDE e não CDE, a segmentação se torna cada vez mais complexa. Essa complexidade não está limitada a hipervisores compartilhados; todas as camadas da infraestrutura que poderiam fornecer um ponto de entrada para um CDE devem ser incluídas ao verificar a segmentação.

Em um ambiente de nuvem privada, uma abordagem que poderá ajudar a reduzir a complexidade dos esforços de segmentação poderia ser localizar todos os componentes virtuais de CDE em um hipervisor de CDE exclusivo e garantir que todos os componentes virtuais não CDE estejam localizados em hipervisores separados, adequadamente segmentados a partir do hipervisor de CDE.

A necessidade de segmentação adequada dos ambientes do cliente em uma nuvem pública ou compartilhada é enfatizada pelo princípio de que os outros ambientes de nuvem de locatários executados na mesma infraestrutura compartilhada devem ser considerados redes não confiáveis. O cliente não tem como confirmar se outros ambientes de nuvem de locatários estão configurados com segurança ou são corrigidos de forma adequada para proteger contra ataques, ou que ainda não estão comprometidos ou até mesmo que não foram projetados para serem maliciosos. Isso é especialmente relevante quando um provedor oferece serviços IaaS e PaaS, pois os clientes individuais têm maior controle e gerenciamento dos seus ambientes.

4.4.2 Responsabilidades de segmentação

Por fim, o provedor precisa assumir a responsabilidade pela segmentação entre os clientes e verificar se ela é eficaz e fornece o isolamento adequado entre os ambientes individuais do cliente, entre os ambientes do cliente e o próprio ambiente do provedor, e entre os ambientes do cliente e outros ambientes não confiáveis (como a internet). Os controles aplicáveis do PCI DSS para as funções de segmentação também seriam a responsabilidade do provedor (por exemplo, regras de firewall, registros de auditoria, documentação, análises etc.). O cliente é responsável pela configuração adequada de quaisquer controles de segmentação implementados dentro do seu próprio ambiente (por exemplo, usando firewalls virtuais para separar VMs dentro do escopo de VMs fora do escopo) e por garantir que o isolamento efetivo seja mantido entre componentes dentro e fora do escopo. O provedor deve testar e relatar controles de segurança que isolam redes entre si de acordo com o Requisito 11.3.4 do PCI DSS.

Os clientes que desejam implementar a segmentação dentro dos seus ambientes de nuvem também precisam considerar como o ambiente e os processos do provedor poderão afetar a eficácia da segmentação. Por exemplo, os sistemas do provedor poderão fornecer conectividade entre as próprias VMs do cliente que não são visíveis para o cliente. Os clientes também devem considerar como o provedor gerencia VMs off-line ou inativas, e se VMs dentro e fora do escopo possivelmente poderiam ser armazenadas em conjunto pelo provedor sem controles ativos de segmentação.

4.4.3 Tecnologias de segmentação

As tecnologias tradicionais de segmentação de rede consistem em dispositivos de hardware como firewalls, switches, roteadores, entre outros. Esses componentes físicos poderiam ser usados para separar VMs hospedadas no mesmo hipervisor ou em múltiplos hipervisores, semelhante a como os sistemas poderiam ser segmentados em uma rede física. Isso exigiria hipervisores com múltiplas interfaces de rede e com configurações que atendam aos requisitos do PCI DSS para os vários tipos de hardware de rede. Além disso, agora há contrapartes virtuais de firewalls, switches e roteadores e podem ser incorporadas em um ambiente virtual.

Conforme mencionado acima, uma consideração fundamental é a forma como as camadas comuns (como hipervisores, implementações de contêineres e componentes físicos compartilhados) constituem e até que ponto representam uma superfície de ataque em potencial entre zonas ou clientes.

Exemplos de controles a serem considerados ao avaliar opções de segmentação incluem, entre outros:

- Firewalls e segmentação de rede no nível da infraestrutura
- Firewalls no hipervisor e no nível da VM
- Etiquetagem ou zoneamento de VLAN além dos firewalls
- Redes definidas por software (consulte a Seção E.4, “Redes definidas por software”, para informações adicionais)
- Sistemas de prevenção de invasão no nível do hipervisor, no nível da VM ou em ambos para detectar e bloquear tráfego indesejado
- Ferramentas de prevenção de perda de dados no nível do hipervisor, no nível da VM ou em ambos
- Controles para prevenir comunicações fora da banda ocorrendo através da infraestrutura subjacente
- Isolamento de processos e recursos compartilhados de ambientes de nuvem de locatários
- Isolamento do sistema baseado em contêineres a partir de tecnologias padrão aprovadas pelo setor
- Armazenamentos de dados segmentados para cada cliente
- Autenticação robusta de dois fatores
- Separação de tarefas e supervisão administrativa
- Registro e monitoramento contínuos do tráfego do perímetro, e resposta em tempo real

Os controles de segmentação devem ser testados anualmente (para comerciantes) ou semestralmente (para provedores de serviços) a fim de confirmar a eficácia do isolamento entre os clientes em um ambiente de nuvem multilocatário. O Suplemento de informações *Orientação para testes de penetração* fornece mais orientações sobre controles de segmentação e princípios de testes.¹⁰

4.5 Considerações sobre determinação do escopo

Comerciantes ou outras organizações que desejam armazenar, processar ou transmitir dados de cartões de pagamento em um ambiente de nuvem devem entender claramente o impacto que estender seu CDE na nuvem terá sobre o escopo do PCI DSS. Por exemplo, em uma implantação em nuvem privada, uma organização poderia implementar a segmentação adequada para isolar sistemas dentro do escopo de outros sistemas e serviços, ou poderia considerar sua nuvem privada como estando totalmente dentro do escopo para o PCI DSS. Em uma nuvem pública, o cliente e o provedor precisarão trabalhar em conjunto para definir e verificar os limites do escopo, pois ambas as partes terão sistemas e serviços dentro do escopo.

O Apêndice D inclui Considerações sobre implementação para requisitos do PCI DSS.

¹⁰ Orientação para testes de penetração Grupo de interesse especial e PCI Security Standards Council, *Orientação para testes de penetração*, (PCI SSC, setembro de 2017), https://www.pcisecuritystandards.org/documents/Participation-Testing-Guidance-v1_1.pdf.

As recomendações para minimizar e simplificar o escopo do PCI DSS em um ambiente de nuvem incluem:

- Não armazenar, processar ou transmitir dados de cartões de pagamento na nuvem. Essa é a maneira mais eficaz de reduzir o escopo do PCI DSS em um ambiente de nuvem.
- O uso de soluções P2PE listadas pelo PCI poderá ajudar a reduzir o escopo do PCI DSS. Embora uma solução P2PE listada pelo PCI não elimine completamente a necessidade de validação do PCI DSS do ambiente de aceitação de pagamento, os ambientes back-end do cliente possivelmente poderiam ser considerados fora do escopo.
- Usar outras tecnologias para reduzir a exposição e desvalorizar os dados dos cartões de pagamento, como a tokenização. Os clientes devem estar cientes e compreender o impacto do escopo de várias soluções de criptografia e tokenização baseadas em nuvem¹¹—por exemplo, aquelas soluções terceirizadas para a nuvem, produtos desenvolvidos internamente ou produtos prontos para uso.
 - As soluções baseadas em nuvem de terceiros possivelmente poderiam limitar a exposição do cliente a um número de conta principal (primary account number, PAN) “clear-text”, pois os dados dos cartões de pagamento podem ser armazenados com o provedor e não pelo próprio cliente.
 - As soluções hospedadas internamente, sejam produtos personalizados, produtos com criptografia prontos para uso ou produtos de tokenização, exigem que a entidade proteja os dados armazenados do titular do cartão dentro da solução e provavelmente envolverão criptografia, gerenciamento de chaves e uso de técnicas de segmentação.
- Implementar uma infraestrutura física dedicada que seja usada apenas para o ambiente de nuvem dentro do escopo. O processo de determinação do escopo será simplificado se todas as operações dentro do escopo estiverem limitadas a um conjunto conhecido e definido de componentes físicos e virtuais do sistema que são gerenciados independentemente dos demais componentes. Uma vez definidos, o cliente dependerá da capacidade do provedor para garantir que os limites do escopo sejam mantidos – por exemplo, ao assegurar que todos os controles de segmentação estejam operando de forma eficaz e que quaisquer componentes novos conectados ao ambiente dentro do escopo sejam imediatamente inseridos dentro do escopo e protegidos de maneira adequada. Embora os provedores de serviços sejam obrigados a realizar testes de controles de segmentação semestralmente, testes contínuos em um ambiente de nuvem apresentariam validação dos controles.
- Minimizar a dependência de provedores terceirizados para proteger os dados dos cartões de pagamento. Quanto mais controles de segurança pelos quais o provedor é responsável, possivelmente maior será o escopo do CDE, aumentando, assim, a complexidade envolvida na definição e na manutenção dos limites do CDE.

Garantir que os dados de conta “clear-text” nunca estejam acessíveis na nuvem também poderá ajudar a reduzir o número de requisitos do PCI DSS aplicáveis ao ambiente de nuvem. Por exemplo, o cliente desempenha todas as operações de criptografia e descryptografia, e todas as funções de gerenciamento de chaves¹² em seu próprio data center e usa uma nuvem de terceiros apenas para armazenar ou transmitir dados criptografados. Nessa situação, os dados “clear-text” nunca existiriam no ambiente de nuvem—nem mesmo temporariamente ou na memória. Além disso, o ambiente de nuvem nunca teria acesso a chaves criptográficas ou a processos de gerenciamento de chaves.

¹¹ Determinação do escopo de SIG, força-tarefa para tokenização e PCI Security Standards Council, *Diretrizes de tokenização do PCI DSS*, Seção 3.2, “Maximizando a redução do escopo do PCI DSS” (PCI SSC, agosto de 2011), https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

¹² De acordo com os requisitos do PCI DSS.

Deve-se observar que os dados criptografados ainda estão dentro do escopo para o PCI DSS (geralmente para a entidade que controla ou gerencia os dados criptografados ou as chaves criptográficas¹³) para garantir que os controles aplicáveis estejam em vigor.

No entanto, ao manter todas as operações de criptografia/descriptografia e gerenciamento de chaves isoladas da nuvem, o número de requisitos do PCI DSS que o provedor deve manter poderá ser reduzido, uma vez que esses requisitos serão aplicáveis ao próprio ambiente e ao pessoal do cliente. O provedor ainda estará dentro do escopo para quaisquer requisitos do PCI DSS que ele gerencie em nome do cliente, por exemplo, os controles de acesso gerenciados pelo provedor precisarão ser verificados para garantir que apenas pessoas autorizadas (conforme determinado pelo cliente) tenham acesso aos dados criptografados e que o acesso não seja concedido a pessoas não autorizadas.

Ou, se dados de conta “clear-text” estiverem presentes (por exemplo, na memória) no ambiente de nuvem ou houver a capacidade de recuperar dados de conta (por exemplo, se as chaves de descriptografia e dados criptografados estiverem presentes), todos os requisitos aplicáveis do PCI DSS se aplicariam a esse ambiente.

Para obter mais informações, consulte o Suplemento de informações *Orientação para determinação do escopo e segmentação de rede do PCI DSS*, para compreender mais sobre os princípios de determinação do escopo e segmentação, conforme aplicável ao ambiente do PCI DSS.¹⁴

4.5.1 **Segurança dos sistemas do cliente de serviços em nuvem**

Os sistemas do cliente usados para acessar o ambiente de nuvem, como estação de trabalho, smartphone e dispositivo de Internet das Coisas (Internet of Things, IoT), não devem ser ignorados, pois possivelmente poderiam se tornar elos fracos na estratégia de segurança na nuvem de um cliente. Os clientes precisam garantir que seus sistemas e processos internos não forneçam acesso não autorizado ao ambiente de nuvem. Por exemplo, se uma estação de trabalho do cliente ou outro dispositivo estiver comprometido, um invasor poderá ser capaz de usar credenciais e um canal autorizado para obter acesso ao ambiente de nuvem a partir do sistema comprometido do cliente. Portanto, o cliente precisará garantir que os dispositivos do seu lado estejam devidamente salvaguardados e protegidos contra acesso físico e lógico não autorizado. **Observação:** os sistemas do lado do cliente usados para acessar dados do titular do cartão na nuvem também estariam dentro do escopo para todos os requisitos aplicáveis do PCI DSS.

¹³ Para obter orientação adicional, consulte “Os dados do titular do cartão criptografados estão dentro do escopo do PCI DSS?” nas Perguntas frequentes no site do PCI SSC.

¹⁴ PCI Security Standards Council, *Orientação para determinação do escopo e segmentação de rede do PCI DSS* (PCI SSC, dezembro de 2016), https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

4.5.2 Exemplos de determinação do escopo para diferentes modelos de implantação em nuvem

Para ambientes de nuvem privada, os esforços de segmentação se voltam para isolar componentes de CDE de componentes não CDE para reduzir o número de sistemas dentro do escopo para o PCI DSS. Em ambientes de nuvem pública ou compartilhada, a segmentação entre os locatários da nuvem é fundamental para a segurança de todo o ambiente do cliente e é complementar para qualquer segmentação gerenciada pelo cliente dentro do seu ambiente para fins de determinação do escopo.

Vários exemplos simples de determinação do escopo são apresentados aqui para fornecer orientação.

Situação	Descrição do ambiente	Orientação para determinação do escopo do PCI DSS
Caso 1: nuvem privada hospedada e controlada por entidade buscando conformidade com o PCI DSS, com segmentação	<ul style="list-style-type: none"> Todas as VMs ou contêineres de CDE são hospedados em um único hipervisor/servidor dedicado; as VMs não CDE são hospedadas em hipervisores ou servidores separados. Segmentação validada dos sistemas de CDE a partir de sistemas não CDE usando uma combinação de controles físicos e lógicos.¹⁵ 	O hipervisor, as VMs e os contêineres de CDE, e todos os componentes do sistema que não são segmentados estão dentro do escopo (a segmentação deve ser validada por fornecer isolamento eficaz).
Caso 2: nuvem privada hospedada e controlada por entidade buscando conformidade com o PCI DSS, sem segmentação	<ul style="list-style-type: none"> Todas as VMs ou contêineres estão hospedados em um ou mais hipervisores ou servidores; algumas VMs transmitem, processam ou armazenam dados do titular do cartão e são consideradas sistemas de CDE, e algumas não processam, transmitem ou armazenam dados do titular do cartão ou não são obrigadas a se comunicar com os sistemas de CDE. Sem segmentação de sistemas de CDE a partir de sistemas não CDE. 	Todo o ambiente de nuvem e todos os sistemas conectados estão dentro do escopo e são considerados parte do CDE (semelhante a uma rede plana).

¹⁵ Orientação para testes de penetração Grupo de interesse especial e PCI Security Standards Council, Orientação para testes de penetração, (PCI SSC, setembro de 2017), https://www.pcisecuritystandards.org/documents/Participation-Testing-Guidance-v1_1.pdf.

Situação	Descrição do ambiente	Orientação para determinação do escopo do PCI DSS
Caso 3: provedor terceirizado que hospeda uma nuvem pública em conformidade com o PCI DSS que é compatível com vários clientes, com segmentação validada para ambientes do cliente	<ul style="list-style-type: none"> As VMs poderão estar em um ou vários hipervisores; todos os hipervisores e VMs são configurados pelo provedor para apoiar os requisitos do PCI DSS. Vários clientes são hospedados em cada hipervisor. Um ou mais contêineres executados em um ou mais servidores de orquestração de contêineres dedicados Segmentação validada dos ambientes do cliente usando uma combinação de controles físicos e lógicos 	O provedor é responsável pela conformidade de todos os elementos de cada serviço em nuvem subjacente compatível com o PCI DSS fornecido ao cliente. O escopo de cada cliente incluiria seu próprio ambiente (por exemplo, VMs, aplicativos etc.), a configuração e a gestão do usuário e do sistema dos serviços do provedor (controles de acesso dos clientes etc.) e quaisquer outros elementos não gerenciados pelo provedor. A segmentação deve ser validada de modo a fornecer isolamento eficaz entre os clientes como parte da validação do provedor e poderá exigir validação adicional como parte da validação de cada cliente.
Caso 4: provedor terceirizado que hospeda uma nuvem pública em conformidade com o PCI DSS que é compatível com vários clientes, sem segmentação do cliente	<ul style="list-style-type: none"> As VMs poderão estar em um ou vários hipervisores; todos os hipervisores configurados pelo provedor para apoiar os requisitos do PCI DSS. Vários clientes estão hospedados em cada hipervisor, configuração de VM gerenciada por cada cliente. Os clientes poderão estar executando contêineres isolados que poderão estar em servidores de orquestração. A segmentação entre os ambientes do cliente não é verificada. Todos os sistemas estão dentro do escopo. 	Este não é um ambiente que provavelmente está em conformidade, considerando que todo o serviço em nuvem e todos os ambientes do cliente estão dentro do escopo. Observe que a validação da conformidade com o PCI DSS poderá ser impraticável e inviável, já que todos os ambientes do cliente precisariam ser incluídos na avaliação (inclusive aplicativos e softwares do cliente). Testes de penetração também precisariam ser realizados para todos os ambientes do cliente. Devido a requisitos regulatórios e de confidencialidade, os clientes em nuvem individuais raramente terão direitos contratuais de auditoria para concluir uma avaliação do PCI DSS que inclua outros clientes.

Situação	Descrição do ambiente	Orientação para determinação do escopo do PCI DSS
<p>Caso 5: nuvem híbrida – o cliente está utilizando um provedor terceirizado que hospeda uma nuvem pública em conformidade com o PCI DSS que é compatível com vários clientes, mas também tem conectividade com uma combinação de nuvem privada hospedada por terceiros ou internamente, ou ambiente hospedado nas dependências do cliente que utiliza serviços e conectividade direta entre essas diferentes plataformas/ambientes.</p>	<ul style="list-style-type: none"> As VMs poderão estar em um ou vários hipervisores. Os hipervisores provavelmente serão configurados pelo provedor para atender aos requisitos do PCI DSS e poderão ter hipervisores gerenciados pelo cliente se houver conectividade para o ambiente local do cliente. Vários clientes são hospedados em cada hipervisor do provedor. O ambiente de nuvem privada ou local do cliente seria dedicado ao cliente. Um ou mais contêineres executados em um ou mais servidores de orquestração de contêineres dedicados Os provedores poderão fornecer serviços utilizados para a conectividade do ambiente de plataforma mista que deve ser incluído como parte da sua validação anual. 	<p>Orientação para determinação do escopo para o provedor O provedor é responsável pela conformidade de todos os elementos do serviço em nuvem que ele oferece. O escopo de cada cliente incluiria seu próprio ambiente (por exemplo, VMs, aplicativos, serviços etc.) e quaisquer outros elementos não gerenciados pelo provedor. Se o provedor fornece os serviços que permitem a conectividade entre os ambientes mistos, então essa solução e o equipamento e o serviço gerenciados pelo provedor deverão ser validados pelo provedor.</p> <p>Ou, se, por exemplo, o provedor permitir que os serviços (físicos ou virtuais) sejam configurados e gerenciados pelo cliente, possibilitando a conectividade entre ambientes mistos, então o escopo do cliente incluiria todas as configurações gerenciadas pelo cliente, enquanto a infraestrutura subjacente seria validada pelo provedor. Os controles de segmentação utilizados na nuvem fornecida pelo provedor devem ser validados por fornecer isolamento eficaz entre clientes como parte da validação do provedor.</p> <p>Orientação de escopo para o cliente - o cliente é responsável por garantir que as soluções e os serviços fornecidos pelo seu provedor para conectividade tenham sido validados em relação à conformidade.</p> <p>O cliente seria responsável pela conformidade de todos os elementos que ele configura e gerencia no ambiente do provedor e em qualquer nuvem no local ou privada conectada ao CDE.</p> <p>O cliente é responsável por garantir que qualquer conectividade entre o provedor e qualquer nuvem privada ou ambientes no local esteja devidamente protegida.</p> <p>O cliente deve validar que todos os controles de segmentação utilizados são eficazes e isolar adequadamente o CDE em todos os ambientes da plataforma mista/híbrida.</p>

Situação	Descrição do ambiente	Orientação para determinação do escopo do PCI DSS
<p>Caso 6: o provedor está prestando serviços de segurança (autenticação, autorização, auditoria etc.) para sistemas CDE no local ou hospedados que poderiam afetar a segurança do CDE (por exemplo, serviço de autenticação e de autorização, permitindo acesso aos dados do titular do cartão).</p>	<ul style="list-style-type: none"> VMs de IaaS/PaaS configuradas pelo cliente em nuvem com serviços de segurança personalizados para atender aos requisitos do PCI DSS 	<p>O cliente é responsável pela conformidade com base na matriz de responsabilidades acordada com o provedor para mantê-lo em conformidade com o PCI DSS. A matriz deve ser incluída como parte da validação do cliente e do provedor.</p>

5 Desafios de conformidade do PCI DSS

As arquiteturas distribuídas de ambientes em nuvem adicionam camadas de tecnologia e complexidade que desafiam os métodos de avaliação tradicionais. Como resultado, pode ser particularmente desafiador validar a conformidade do PCI DSS em uma infraestrutura dinâmica e distribuída, como um ambiente público ou de vários clientes. Exemplos de desafios de conformidade incluem, entre outros, os seguintes:

- Os clientes podem ter pouca ou nenhuma visibilidade da infraestrutura subjacente do provedor e dos controles de segurança relacionados, o que dificulta identificar quais componentes do sistema estão dentro do escopo para um serviço específico ou quem é responsável pelos controles específicos do PCI DSS.
- Os clientes podem ter supervisão limitada ou nenhuma supervisão ou controle sobre o armazenamento de dados do titular do cartão. As organizações podem não saber onde os dados do titular do cartão são armazenados fisicamente ou os locais podem mudar regularmente. Por motivo de redundância ou de alta disponibilidade, os dados poderiam ser armazenados em vários locais a qualquer momento.
- Pode ser difícil determinar um tamanho de amostragem apropriado para ambientes de nuvem e processos dinâmicos que mudam rapidamente (por exemplo, cloud-bursting, implantação contínua e terminação de máquinas virtuais, endereçamento IP dinâmico, entre outros).
- Alguns componentes virtuais não têm os mesmos níveis de controle de acesso, registro e monitoramento que suas contrapartes físicas.
- Os limites do perímetro entre os ambientes do cliente podem ser fluidos.
- Os ambientes de nuvem pública geralmente são projetados para permitir acesso a partir de qualquer lugar na internet.
- Pode ser desafiador verificar quem tem acesso aos dados do titular do cartão processados, transmitidos ou armazenados no ambiente de nuvem.
- Pode ser desafiador coletar, correlacionar e arquivar todos os registros necessários para atender aos requisitos aplicáveis do PCI DSS.
- Organizações que usam ferramentas de descoberta de dados para identificar dados do titular do cartão em seus ambientes e garantir que tais dados não sejam armazenados em locais inesperados poderão descobrir que a execução dessas ferramentas em um ambiente de nuvem pode ser difícil e gerar resultados incompletos. Pode ser desafiador para as organizações verificar se os dados do cartão do titular não "vazaram" na nuvem.
- Nem todos os serviços oferecidos por um provedor podem ser incluídos na validação de conformidade do PCI DSS do provedor. Muitos provedores podem não apoiar o direito de auditar seus clientes.

Esses desafios afetarão diversos fatores relacionados ao modo como a conformidade com o PCI DSS é gerenciada, incluindo como a segmentação é implementada, como as avaliações do PCI DSS são abrangidas, como os requisitos individuais do PCI DSS são validados e qual parte desempenhará atividades de validação específicas.

Em um nível alto, os provedores podem ser identificados como aqueles que foram validados por atender a um nível específico de conformidade com o PCI DSS e aqueles que não atenderam. A prática recomendada para clientes com considerações do PCI DSS é trabalhar com provedores cujos serviços foram validados independentemente como sendo compatíveis com o PCI DSS e têm mecanismos disponíveis para os clientes para obter tal evidência.

5.1 O que significa quando um provedor afirma: "estou em conformidade com o PCI DSS"?

Confia-se bastante na afirmação "estou em conformidade com o PCI DSS", mas o que isso realmente significa para as diferentes partes envolvidas?

O uso de um provedor compatível com o PCI DSS não resulta automaticamente em conformidade com o PCI DSS para os clientes. O cliente deve confirmar que o provedor está em conformidade com o PCI DSS e que os serviços usados pelo cliente foram incluídos na validação de conformidade do PCI DSS do provedor (consulte a Seção 5.2, "Verificação do escopo dos serviços e componentes validados do PCI DSS"). Além disso, o cliente ainda deve garantir que esteja usando o serviço de forma compatível e também é responsável pela segurança de seu CHD – terceirizar o gerenciamento diário de um subconjunto de requisitos do PCI DSS não elimina a responsabilidade do cliente de garantir que o CHD esteja devidamente protegido e que os controles do PCI DSS sejam atendidos. Portanto, o cliente deve trabalhar com o provedor para garantir que evidências sejam fornecidas para verificar se os controles do PCI DSS são mantidos continuamente. Um Atestado de conformidade (Attestation of Compliance, AOC) reflete apenas um momento específico isolado; entretanto, manter a conformidade exige monitoramento contínuo e confirmação periódica (por exemplo, pelo menos uma vez por ano) de que os controles estão em vigor e funcionando de forma eficaz.

Mesmo que um serviço em nuvem seja validado para determinados requisitos do PCI DSS, essa validação não é automaticamente transferida para os ambientes do cliente dentro do serviço em nuvem. Por exemplo, a validação de um provedor pode ter incluído o uso de software antivírus atualizado nos sistemas do provedor; entretanto, esta validação pode não se estender ao Sistema operacional ou às VMs do cliente individual (como em um serviço IaaS). Além disso, o cliente ainda deve manter a conformidade em relação a todas as suas próprias operações, por exemplo, ao garantir que o antivírus seja instalado e atualizado em todos os sistemas do lado do cliente usados para se conectar ao ambiente de nuvem.

Da mesma forma, a conformidade do PCI DSS do cliente não resulta em nenhuma reivindicação de conformidade para o provedor, mesmo que a validação do cliente inclua elementos do serviço gerenciado pelo provedor. Como resultado, um cliente deve confirmar que os serviços fornecidos pelo provedor apoiam sua conformidade com o PCI DSS.

Em relação à aplicabilidade da conformidade do PCI DSS de uma parte com a outra, considere o seguinte:

- Se um provedor estiver em conformidade, isso não significa que seus clientes estejam.
- Se um ou mais dos clientes do provedor estiverem em conformidade, isso não significa que o provedor esteja em conformidade.
- Se um provedor e o cliente estiverem em conformidade, isso não significa que os demais clientes estejam.

O provedor deve garantir que qualquer serviço oferecido como estando em conformidade com o PCI DSS seja acompanhado por uma explicação clara e inequívoca, respaldada por evidências apropriadas, detalhando quais aspectos do serviço foram validados como estando em conformidade e quais não foram.

5.2 Verificação do escopo dos serviços e componentes validados do PCI DSS

Os clientes precisarão obter detalhes da validação de conformidade do PCI DSS do provedor para determinar se o serviço que estão usando está totalmente coberto. Os provedores que validaram a conformidade com o PCI DSS podem ou não ser incluídos em uma lista publicada por uma bandeira de cartão de pagamento; entretanto, todos os provedores validados pelo PCI DSS devem ser capazes de fornecer um AOC detalhando os serviços e locais incluídos na validação de conformidade do PCI DSS.

As perguntas a seguir podem ser úteis para os clientes fazerem aos seus provedores:

- Há quanto tempo o provedor está em conformidade com o PCI DSS? Quando foi sua última validação?
- Quais serviços específicos foram incluídos na validação?
- Para cada serviço usado pelo cliente, quais requisitos do PCI DSS foram incluídos na validação?
- A validação de conformidade foi realizada por um avaliador qualificado e treinado pelo PCI (por exemplo, QSA ou ISA)?
- O provedor forneceu informações (por exemplo, uma matriz de responsabilidades) para clientes que claramente delineiam os requisitos do PCI DSS atendidos em nome do cliente?
- Quais serviços, instalações e componentes do sistema específicos foram incluídos na validação?
- Há algum componente do sistema com o qual o provedor conta para a entrega do serviço que não foi incluído na validação do PCI DSS?
- Como o provedor garante que os clientes que usam o serviço compatível com PCI DSS não sejam capazes de introduzir componentes não compatíveis com o ambiente ou ignorar quaisquer controles do PCI DSS?

Os provedores devem fornecer aos seus clientes evidências que identifiquem claramente o escopo de sua avaliação do PCI DSS, os requisitos específicos do PCI DSS em relação aos quais o ambiente foi avaliado e a data da avaliação. O cliente deve ter uma compreensão detalhada de quaisquer requisitos de segurança que não sejam cobertos pelo provedor e, portanto, é responsabilidade do cliente implementar, gerenciar e validar como parte de sua própria conformidade com o PCI DSS. O cliente deve discutir suas necessidades com o provedor para determinar como o provedor pode fornecer garantia de que os controles necessários estão em vigor.

Os provedores que passaram por avaliação do PCI DSS para validar sua conformidade terão os resultados resumidos em um AOC e detalhados em um Relatório de conformidade (Report on Compliance, ROC) ou um Questionário de autoavaliação (Self-Assessment Questionnaire, SAQ) D para provedores de serviços. As seções Resumo executivo e Escopo de trabalho do ROC devem detalhar o escopo da avaliação, incluindo os componentes, as instalações e os serviços específicos que foram avaliados. A avaliação e o atestado por parte de um avaliador qualificado e treinado pelo PCI fornecem níveis mais altos de garantia de que os requisitos do PCI DSS foram compreendidos e os procedimentos de teste foram seguidos. Se a avaliação de um provedor não tiver sido realizada por um avaliador qualificado e treinado pelo PCI, o cliente poderá querer fazer perguntas adicionais sobre o rigor da avaliação, a qualificação do avaliador, entre outras.

5.3 Verificação dos controles do PCI DSS gerenciados pelo provedor de serviços em nuvem

Assim como ocorre com todos os serviços hospedados dentro do escopo do PCI DSS, o cliente deve solicitar ao seu provedor evidência e garantia suficientes de que todos os processos e componentes dentro do escopo sob o controle do provedor são compatíveis com o PCI DSS. Essa verificação pode ser concluída pelo avaliador do cliente (como um QSA ou ISA) como parte da avaliação do PCI DSS do cliente. Se o provedor já passou por uma avaliação do PCI DSS que foi realizada por outro avaliador, o avaliador do cliente precisará verificar se a validação do provedor é atual, se a avaliação abrangeu todos os serviços prestados ou usados pelo cliente e se todos os requisitos aplicáveis foram considerados em vigor para os ambientes e os sistemas dentro do escopo.

Os provedores que passaram pela avaliação e validação de conformidade do PCI DSS devem ser capazes de fornecer aos seus clientes o seguinte:

- Documentação de comprovação de conformidade (como o AOC e as seções aplicáveis do ROC), incluindo a data da avaliação de conformidade
- Evidência documentada dos componentes e serviços do sistema que foram incluídos na avaliação do PCI DSS (conforme aplicável ao serviço)
- Evidência documentada dos componentes e serviços do sistema que foram excluídos na avaliação do PCI DSS (conforme aplicável ao serviço)
- Evidência documentada (como o AOC e seções aplicáveis do ROC) de controles de compensação que foram usados para atender a qualquer um dos requisitos do PCI DSS
- Linguagem contratual apropriada (de acordo com os requisitos 12.8.2 e 12.9 do PCI DSS)

Os provedores que não passaram pela avaliação de conformidade do PCI DSS precisarão ser incluídos na avaliação do seu cliente. O provedor precisará concordar em fornecer ao avaliador do cliente (ou seja, um ISA ou um QSA) acesso ao seu ambiente ou a um ambiente gerenciado por um provedor de serviços terceirizado (consulte a Seção 3.4, “Relacionamentos com provedores de serviços aninhados”) para que o cliente conclua sua avaliação. O avaliador do cliente pode exigir acesso no local e informações detalhadas do provedor, incluindo, entre outras:

- Acesso a sistemas, instalações e pessoal apropriado para revisões no local, entrevistas, avaliações físicas etc.
- Políticas e procedimentos, documentação de processos, padrões de configuração, registros de treinamento, planos de resposta a incidentes etc.
- Evidência (como configurações, capturas de tela, relatórios de testes de segmentação, revisões de processo etc.) para mostrar que todos os requisitos aplicáveis do PCI DSS estão sendo atendidos para os componentes do sistema dentro do escopo
- Linguagem contratual apropriada (de acordo com os requisitos 12.8.2 e 12.9 do PCI DSS)

O cliente e o provedor precisarão concordar sobre quais atividades de avaliação podem ser realizadas pelo cliente e quais testes são de responsabilidade do provedor. Por exemplo, em um serviço IaaS/PaaS, o cliente pode querer testar dentro de seu próprio ambiente e qualquer outro tipo de acesso, como os limites entre si e outros clientes, ou entre si e os sistemas do provedor. No entanto, se tais testes não forem permitidos pelo provedor, o cliente terá de contar com o provedor para executar e validar esses requisitos. Em ambientes SaaS, o cliente terá visibilidade limitada ou nenhuma visibilidade nem permissão para realizar testes e, em geral, dependerá do provedor para todos os testes e validação. As atividades de teste definidas e seus controles e permissões associadas devem ser detalhados no SLA.

Preferencialmente, o provedor deve ser capaz de fornecer aos clientes detalhes específicos, conforme aplicável à manutenção contínua da conformidade com o PCI DSS. Por exemplo, dependendo do serviço fornecido, o provedor poderia fornecer cópias de arquivos de registro, registros de atualização de patch ou conjuntos de regras de firewall que se aplicam especificamente ao ambiente de um cliente individual.

Os provedores que desejam fornecer um serviço compatível com o PCI DSS podem querer isolar os serviços compatíveis com o PCI DSS de seus serviços compatíveis com o PCI DSS. Isso pode ajudar a simplificar o processo de validação de conformidade para o provedor e para seus clientes individuais. Também pode ajudar o provedor a padronizar os serviços compatíveis com o PCI DSS sendo fornecidos aos seus clientes.

6 Considerações sobre segurança

Embora o uso de serviços em nuvem possa proporcionar uma oportunidade atraente para organizações de todos os portes terceirizarem e utilizarem recursos de segurança gerenciados centralmente, as organizações também devem estar cientes dos riscos e desafios associados a uma determinada escolha de nuvem antes de migrar seus dados ou serviços confidenciais para o ambiente de nuvem. Esta seção explora algumas dessas considerações adicionais de segurança.

6.1 Governança, risco e conformidade

Um desafio básico em relação a ambientes de nuvem é o gerenciamento da governança, do risco e da conformidade, que geralmente é uma responsabilidade compartilhada entre o cliente e o provedor. Na segurança, o compartilhamento passa por escrutínio rigoroso para esclarecer a responsabilidade e a prestação de contas quanto ao desempenho de determinadas atividades de controle. O delineamento das responsabilidades enfatiza a importância de uma sólida governança, estrutura de gestão de riscos e SLAs. Sem uma estratégia de governança clara, o cliente pode não estar ciente de problemas decorrentes do uso do serviço em nuvem, e o provedor pode não estar ciente de problemas dentro do ambiente do cliente que possam afetar a prestação de seu serviço. Durante a determinação do escopo da nuvem, é fundamental incluir as interfaces internas e externas da arquitetura de segurança e demarcar os limites que representam o domínio de governança do usuário da nuvem e do provedor.

Uma matriz de responsabilidades seria uma abordagem adequada para definir com clareza a estratégia de governança na nuvem, particularmente quando documentada no SLA. Isso permite que haja clareza das responsabilidades entre o cliente e o provedor quanto à segurança operacional e à gestão de risco. Os mecanismos de notificação e monitoramento devem ser disponibilizados pelo provedor para que seus clientes forneçam garantia de que a governança eficaz seja aplicada e mantida pelo provedor durante a vigência do serviço. Exemplos de relatórios incluem, entre outros:

- Relatórios de auditoria interna
- Relatórios de auditoria independente
- Relatórios de testes de vulnerabilidades e penetração
- Plano de ação de remediação de riscos e vulnerabilidades

6.1.1 Gestão de risco

Consistente com uma abordagem de gestão de risco para serviços internos, os serviços de nuvem terceirizados devem ser avaliados quanto à estratégia de risco de uma organização com a intenção de identificar ativos críticos, analisar possíveis riscos para esses ativos e desenvolver um plano de tratamento de risco apropriado.

Em ambientes tradicionais, a localização física dos dados confidenciais pode ser restrita a sistemas dedicados e jurisdições, facilitando a identificação e a implementação de controles eficazes de mitigação de riscos. No entanto, o advento de novas tecnologias exige uma reavaliação das estratégias de risco tradicionais. Por exemplo, os dados em ambientes de nuvem não estão mais vinculados a um sistema ou local físico, reduzindo a eficácia dos mecanismos de segurança tradicionais para proteger os dados contra riscos. Abordagens de segurança tradicionais que criam controles de segurança para proteger dados confidenciais podem, portanto, precisar evoluir para abordar esse ambiente de risco emergente.

Do mesmo modo, as formas tradicionais de avaliação de risco podem não levar em consideração características específicas da nuvem, como um modelo de pagamento por uso ou multilocatário (descrito na Seção E2, “Multilocatário”) e podem, portanto, exigir procedimentos novos ou modificados.

6.1.2 Devida diligência

Um provedor que armazena, processa ou transmite dados do titular do cartão, ou que pode afetar a segurança do cliente de outra forma seria considerado um provedor de serviços terceirizado do cliente. Assim como ocorre com todos os provedores de serviços, os clientes devem seguir um processo completo de devida diligência (consulte o Requisito 12.8 do PCI DSS) antes de contratar o provedor. O processo específico de devida diligência e as metas variarão para cada cliente; no entanto, os objetivos comuns normalmente incluem:

- Confirmar que o provedor tem um histórico de boas práticas de trabalho e comportamento ético, e está realizando legitimamente os serviços que o cliente acredita que sejam
- Compreender as responsabilidades operacionais do provedor, como resposta a incidentes, criptografia e monitoramento da segurança
- Verificar se o provedor é compatível com a imagem comercial e o perfil de risco do cliente
- Identificar possíveis riscos ou circunstâncias associadas ao provedor que possam afetar as operações ou os negócios do cliente
- Identificar elementos do serviço que precisam ser esclarecidos e incluídos em contratos ou SLAs

A devida diligência eficaz não lê simplesmente o material de marketing do provedor ou se baseia nas declarações do provedor sobre a conformidade com o PCI; em vez disso, envolve pesquisa, análise e coleta de evidências. Os clientes devem ter a certeza de que estão contratando um provedor que possa atender às suas necessidades de segurança e operacionais antes de assumir tais compromissos. O escopo do exercício de devida diligência deve considerar, no mínimo, os tópicos discutidos ao longo deste documento, conforme aplicável aos requisitos específicos do cliente.

Realizar um exercício de devida diligência antes da contratação do provedor não elimina a necessidade de realizar um monitoramento contínuo e a revisão dos serviços oferecidos pelo provedor.

6.1.3 Acordos de nível de serviço

O uso de serviços em nuvem inclui a implantação de um modelo de serviço definido e deve ser sempre sobrescrito por SLAs abrangentes que estejam em conformidade com os padrões internacionais para SLAs de computação em nuvem, incluindo ISO/IEC 19086-1:2016 Tecnologia da informação -- Computação em nuvem -- Estrutura de acordo de nível de serviço (Service level agreement, SLA) -- Parte 1: Visão geral e conceitos. A entrega segura de qualquer serviço em nuvem depende do pessoal, dos processos e das tecnologias do provedor, enquanto o uso seguro dos serviços em nuvem permanece sendo responsabilidade do cliente.

Normalmente, os contratos de hospedagem em nuvem estão preocupados com o “tempo de funcionamento” e a alta disponibilidade, com pouca ou nenhuma menção ou garantia de integridade e de segurança dos dados. No entanto, o cliente é responsável por garantir que o serviço que está usando atenda aos seus requisitos de integridade e de segurança dos dados e obrigações de conformidade.

Os SLAs e outros acordos por escrito entre o provedor e o cliente devem identificar claramente a descrição das responsabilidades entre as partes, incluindo responsabilidades pela implementação e gestão de diferentes controles de segurança. Esses SLAs formam os componentes fundamentais de como as operações e a segurança serão realizadas e, como resultado, devem ser estabelecidos como um pré-requisito para qualquer implementação de serviço em nuvem. As atividades de validação e teste de conformidade do PCI DSS (com os controles, as permissões e os cronogramas associados) também devem ser claramente detalhadas no SLA.

A não elaboração e concordância quanto a SLAs apropriados podem resultar em problemas para o cliente se o serviço em nuvem não atender às necessidades e demandas do seu negócio. Os SLAs devem ser estabelecidos e acordados como parte de quaisquer negociações contratuais e de serviço. O desempenho, a disponibilidade, a integridade e a confidencialidade devem ser considerados, e SLAs devem ser acordados para cada serviço gerenciado ou operado pelo provedor. Acordos por escrito também devem abranger as atividades e garantias a serem fornecidas por ambas as partes após a rescisão da prestação de serviços.

6.1.4 Planos de continuidade de negócios e recuperação de desastres

Os requisitos organizacionais para planos de continuidade de negócios (business continuity plans, BCP), tolerância a falhas, alta disponibilidade e controles de recuperação de desastres (disaster recovery, DR) se aplicam aos ambientes terceirizados do cliente, bem como a instalações gerenciadas pelo cliente. Os clientes devem considerar se os procedimentos de continuidade e de recuperação do provedor são suficientes para atender aos requisitos organizacionais do cliente, e o escopo do PCI DSS do serviço em nuvem deve incluir quaisquer sites e sistemas de tolerância a falha que possam ser usados para armazenar, processar ou transmitir dados do titular do cartão em uma situação de BCP ou de DR. A capacidade de realizar testes das capacidades de BCP e de DR e de observar os resultados dos testes do provedor também deve ser considerada.

6.1.5 Recursos humanos

O gerenciamento dos recursos humanos do provedor está totalmente fora do controle do cliente. Os processos de devida diligência do cliente devem incluir uma compreensão dos recursos humanos do provedor e práticas contínuas de treinamento de conscientização de segurança da informação. Os Requisitos 12.6 e 12.7 do PCI DSS fornecem uma base para avaliar o processo de triagem de contratação e o programa de treinamento de conscientização de segurança do provedor.

6.2 Instalações e segurança física

Os serviços em nuvem envolvem recursos físicos localizados no ambiente do provedor (incluindo a infraestrutura de DR discutida acima) que são acessados remotamente a partir do ambiente do cliente. Semelhante a outros provedores terceirizados, os provedores de nuvens públicas e compartilhadas prestam serviços para vários clientes cujos dados e componentes virtuais coexistem no mesmo local físico e são gerenciados pelos mesmos sistemas físicos que os de outros clientes. Para uma instalação do provedor, controles de segurança física precisam ser implementados para proteger a infraestrutura do provedor, bem como os dados dos clientes. Para provedores validados pelo PCI DSS, o AOC deve incluir uma lista de todos os locais físicos que foram avaliados como parte da validação de conformidade do PCI DSS.

Em uma nuvem privada, a localização física de todos os componentes é conhecida e pode ser verificada. Ao usar uma nuvem pública, diferentes elementos do ambiente, como VMs, hipervisores, dispositivos de rede virtual etc., podem ser frequentemente realocados de acordo com a estratégia de entrega de serviços do provedor (por exemplo, distribuição de carga, tolerância a falhas, alta disponibilidade) em vários locais físicos. Verificar se a segurança física apropriada está em vigor pode ser desafiador em um ambiente onde os dados e a infraestrutura podem estar em vários locais diferentes em diferentes momentos. Um cliente deve garantir que seus requisitos de segurança física sejam aplicados de forma consistente em todos os locais em potencial.

6.3 Considerações sobre segurança de dados

O diagrama a seguir mostra uma representação típica do ciclo de vida dos dados:¹⁶



Figura 3. O ciclo de vida típico dos dados

É importante identificar e definir os dados usados e produzidos em seu ambiente e como os aspectos de segurança são gerenciados ao longo de seu ciclo de vida. Para todas as categorias de serviço em nuvem, requisitos claros relacionados à retenção, ao armazenamento e ao descarte seguro de dados devem compor o processo de contratação para garantir que os dados confidenciais:

- Sejam retidos pelo tempo necessário
- Não sejam retidos por mais tempo do que o necessário
- Sejam armazenados apenas em locais apropriados e protegidos
- Estejam acessíveis apenas para pessoas com necessidade comercial
- Sejam processados de acordo com a política de segurança do cliente

6.3.1 Aquisição de dados

O cliente determinará, em última instância, como e quando os dados do titular do cartão são adquiridos no ambiente de nuvem. Processos de ponta a ponta e fluxos de dados devem ser documentados nas redes do cliente e do provedor de modo que seja claramente compreendido onde os dados do titular do cartão estão localizados e como estão cruzando a infraestrutura (consulte o Requisito 1.1.2 do PCI DSS). Isso também ajudará o cliente e o provedor a identificar onde cada entidade adquire e para onde envia os dados do titular do cartão ao longo do processo.

¹⁶ Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0* (Cloud Security Alliance, 2017). <https://cloudsecurityalliance.org/download/security-guidance-v4>.

6.3.1.1 Classificação de dados

A classificação de dados e a gestão de dados de acordo com sua classificação variarão de organização para organização. Um sistema de classificação de dados definido pode ajudar as organizações a identificar dados confidenciais ou confidenciais e dados com necessidades de segurança específicas. Isso, por sua vez, permite que as organizações atribuam mecanismos de proteção adequados com base nas necessidades de segurança de diferentes tipos de dados e ajuda a evitar que dados confidenciais sejam processados inadvertidamente ou tratados como não confidenciais.

6.3.1.2 Migração para um ambiente de nuvem

Recomenda-se que as necessidades de segurança de dados sejam avaliadas para todos os tipos de informações migradas para um ambiente de nuvem, não apenas os dados do titular do cartão. Por exemplo, dados operacionais, políticas e procedimentos de segurança, configurações do sistema e padrões de construção, arquivos de registro, relatórios de auditoria, credenciais de autenticação, chaves criptográficas, planos de resposta a incidentes e detalhes de contato de funcionários são apenas alguns dos tipos de dados com diferentes requisitos de segurança que talvez precisem ser considerados. Se os processos de segurança de dados não forem claramente definidos e documentados, os dados podem ser expostos involuntariamente ou estar sujeitos a riscos desnecessários que poderiam resultar em perda ou divulgação inadequada.

6.3.1.3 Soberania dos dados e considerações legais

Dependendo do modelo de implantação e da categoria de serviço em nuvem adotada, e devido à natureza dinâmica das operações em nuvem, talvez não se saiba onde informações específicas realmente residem. Isso pode resultar em preocupações sobre a propriedade dos dados e possíveis conflitos entre requisitos legais e regulatórios nacionais ou internacionais. Por exemplo, a infraestrutura do provedor pode resultar em dados percorrendo ou sendo armazenados em países política ou economicamente instáveis, ou estando sujeitos a regulamentações regionais.

Compreender as jurisdições legais que se aplicam a dados em diferentes países ou regiões pode ser um desafio para o cliente. Por exemplo, os clientes sujeitos a leis regionais que restringem fluxos transfronteiriços de dados precisarão verificar todos os locais e fluxos de seus dados para garantir que seus serviços em nuvem estejam em conformidade com suas obrigações legais.

Outras considerações legais incluem requisitos relacionados à descoberta eletrônica, preservação e integridade de evidências, e custódia de dados. Os provedores devem ter processos documentados para responder a solicitações legais de apreensão de registros, incluindo registros de dados/de auditoria pertencentes ao provedor e seus clientes. Os clientes devem entender as ramificações de tais leis nos países onde seus dados estão presentes, bem como os processos nos quais seu provedor se envolverá.

Além das considerações sobre soberania dos dados mencionadas acima, os provedores públicos frequentemente têm vários sistemas de armazenamento de dados localizados em vários data centers que muitas vezes poderão estar em vários países ou regiões. Consequentemente, o cliente pode não saber a localização de seus dados ou os dados podem estar presentes em um ou mais dos vários locais em qualquer momento específico. Além disso, um cliente pode ter pouca ou nenhuma visibilidade dos controles que protegem seus dados armazenados. Isso pode tornar a validação da segurança de dados e dos controles de acesso para um conjunto de dados específico particularmente desafiadora.

6.3.2 Armazenamento e persistência de dados

Além da gama conhecida de locais de armazenamento pretendidos, os dados também podem estar presentes em outros sistemas do provedor usados para a manutenção da infraestrutura de nuvem, como imagens de VM, backups, registros de monitoramento, entre outros. Os dados do titular do cartão armazenados na memória também poderiam ser gravados no disco para fins de recuperação ou de alta disponibilidade (por exemplo, no caso de suspensão ou snapshot da máquina virtual). Esses dados armazenados poderão ser facilmente esquecidos e, portanto, não protegidos pelos controles de segurança de dados. Todos os pontos de captura em potencial devem ser identificados e gerenciados conforme necessário para prevenir o armazenamento não intencional ou inseguro ou, ainda, a transmissão de dados confidenciais. Ferramentas e processos especializados podem ser necessários para localizar e gerenciar dados armazenados em imagens arquivadas, offline ou reposicionadas.

O possível acesso do hipervisor aos dados na memória também deve ser levado em consideração para garantir que os controles de acesso definidos pelo cliente não sejam ignorados involuntariamente pelo pessoal do administrador do provedor.

As organizações devem garantir que suas necessidades específicas de segurança de dados possam ser atendidas pelo serviço em nuvem antes de migrar esses dados para o ambiente de nuvem. As considerações devem incluir como o armazenamento de tipos de dados com diferentes níveis de confidencialidade no mesmo ambiente virtual pode afetar os níveis de proteção necessários para cada tipo de dados. Dados do titular do cartão, credenciais e senhas do usuário, e chaves criptográficas são exemplos de dados confidenciais que devem ser protegidos de acordo com suas necessidades individuais.

6.3.3 Uso de dados

Os dados devem estar acessíveis apenas àquelas pessoas com necessidade comercial e devem ser processados de acordo com a política de segurança da informação estabelecida.

6.3.4 Compartilhamento de dados

Como todos os ambientes fora do ambiente controlado pelo cliente podem ser potencialmente não confiáveis, os serviços em nuvem devem ser compatíveis com a transmissão segura dos dados do titular do cartão em toda a infraestrutura da nuvem, entre os ambientes do cliente e da nuvem, entre os ambientes do cliente e entre a infraestrutura da nuvem e outras redes públicas. Recomenda-se que dados confidenciais sejam criptografados para todas as transmissões através de qualquer ambiente de nuvem que não seja totalmente privado ou controlado pelo cliente. Ambientes de nuvem fora do ambiente controlado pelo cliente devem ser tratados como redes abertas ou públicas (consulte o Requisito 4.1 do PCI DSS).

6.3.5 Descomissionamento e descarte

Em um ambiente de nuvem distribuído, a verificação de que todas as instâncias dos dados do titular do cartão foram excluídas de forma segura de acordo com a política de retenção de dados do cliente está sujeita aos mesmos desafios identificados acima quanto à validação da segurança de dados e dos controles de acesso. O descarte dos dados do titular do cartão deve ser realizado usando métodos seguros de acordo com os requisitos do PCI DSS e todos os locais dos dados do titular do cartão de ambos os ambientes do cliente e do provedor precisam ser incluídos. O método de descarte deve garantir que os dados não sejam recuperáveis após a conclusão do processo de descarte.

Além do descarte de dados, os requisitos de descomissionamento de recursos devem ser definidos para respaldar decisões futuras dos clientes relacionadas à migração para um novo provedor, ao descomissionamento de seus recursos de nuvem ou à saída completa de um ambiente de nuvem.

O provedor deve fornecer mecanismos de descarte de dados que forneçam garantia ao cliente de que todos os dados foram removidos e excluídos com segurança do ambiente de nuvem. Os procedimentos para o encerramento do serviço devem ser claramente definidos e documentados, e considerados no contexto de estar sujeitos a regulamentações regionais.

Os clientes podem optar por garantir que todos os dados sejam criptografados com criptografia forte (consulte as Seções E10, “Criptografia de dados e gerenciamento de chaves criptográficas” e E.11, “Dispositivos de criptografia segura na nuvem” para mais informações) para reduzir o risco de haver quaisquer dados residuais nos sistemas do provedor. No entanto, os clientes devem estar cientes de que deixar quantidades potencialmente desconhecidas de dados criptografados nos sistemas do provedor após o término do acordo provavelmente é uma violação da política de retenção de dados.

6.4 Resposta a incidentes e investigação forense

Resposta a incidentes, procedimentos de encaminhamento e investigações forenses, para garantir o processamento oportuno e eficaz de todos os incidentes de segurança, são essenciais para as operações dos clientes e dos provedores, e são elementos essenciais da conformidade geral com o PCI DSS. No entanto, há diferenças e desafios diferentes no processamento de dados forenses e em como os processos de resposta a incidentes precisarão ser ajustados para cada categoria de serviço em nuvem.

Os clientes devem trabalhar com seus provedores para documentar funções e responsabilidades relacionadas à resposta a incidentes de segurança e à notificação forense e de violação de dados como parte de SLAs e acordos contratuais, levando-se em consideração a necessidade de cumprir com a gestão de incidentes de segurança (ou seja, Requisitos 12.5.3, 12.8.3 e 12.10 do PCI DSS) e com os requisitos do provedor de serviços (ou seja, Requisito 12.9 do PCI DSS).

6.4.1 Resposta a incidentes

Os clientes precisam saber quando um problema, incidente ou violação ocorreu e o impacto sobre seu ambiente ou seus dados. Problemas, incidentes e violações de dados devem ser comunicados pelo provedor a todos os clientes afetados em tempo hábil. Os clientes também devem considerar se o provedor exige que todos os clientes notifiquem imediatamente o provedor sobre possíveis violações em seus ambientes, permitindo que o provedor responda mais rapidamente para conter a violação e minimizar seu impacto para outros clientes. A partir do tipo de categoria de serviço em nuvem usada, relacionada à facilitação de armazenamento, processamento ou transmissão de dados do titular do cartão, cada fase do ciclo de vida de resposta a incidentes (por exemplo, conforme NIST 800-61rev2) é afetada em um nível diferente. (Observe que outras estruturas padrão internacionais referentes à resposta a incidentes são ISO/IEC 27035 e “Estratégias para resposta a incidentes e cooperação para crises cibernéticas” da ENISA.). Definições do que constitui uma violação ou incidente exigindo notificação entre o cliente e o provedor devem ser acordadas. Os processos e prazos de notificação devem ser incluídos nos SLAs, e os planos de resposta a incidentes devem incluir requisitos de notificação. Em alguns casos, a renegociação dos SLAs poderá ser necessária se o tempo de resposta acordado ou a viabilidade das informações críticas para a investigação não for adequado ou suficiente.

6.4.2 Investigação forense

O potencial para que os dados do cliente sejam capturados por terceiros durante uma investigação de violação também deve ser claramente compreendido. A investigação de incidentes pode envolver considerações legais e requisitos de jurisdição, e esses requisitos devem ser incluídos em SLAs ou em acordos operacionais (consulte a Seção 6.3.1.3, “Soberania de dados e considerações legais”).

A funcionalidade forense deve ser especificada nos objetivos de nível de serviço (service level objectives, SLOs) incorporados ao SLA entre o cliente e o provedor. Os SLOs podem incluir requisitos de notificação, identificação, preservação e acesso a possíveis fontes de evidências.¹⁷

Os clientes e as agências de fiscalização exigem e dependem dos provedores para o suporte forense, e essas obrigações variam dependendo da categoria do serviço em nuvem, conforme observado abaixo.¹⁸

- **SaaS:** a capacidade forense depende do suporte do provedor, pois os clientes não têm controle sobre o ambiente do provedor. Os examinadores forenses talvez tenham de contar com registros de aplicativos de alto nível disponíveis a partir do aplicativo SaaS. Os SLOs podem incluir fontes de evidências como registros de aplicativos, Web, servidor de banco de dados, sistema operacional convidado/host, portal, captura de rede e sistemas de faturamento.
- **PaaS:** a capacidade forense é compartilhada entre clientes e provedores. Os clientes controlam o aplicativo de software desenvolvido e hospedado e, portanto, controlam a capacidade forense dentro do aplicativo, o registro automático em um servidor de registro externo pode ser configurado para capturar a trilha de auditoria aplicável. No entanto, como a operação real do aplicativo está dentro da infraestrutura controlada do provedor, os clientes devem identificar claramente as responsabilidades dos provedores com relação à investigação forense. Os SLOs podem incluir fontes de evidências como registros de aplicativos, Web, servidor de banco de dados, sistema operacional convidado/host, portal, captura de rede, e portal de faturamento e gestão.
- **IaaS:** a capacidade forense é compartilhada entre clientes e provedores. Os clientes têm maior controle sobre a gama de possíveis fontes de evidências; entretanto, alguns dados essenciais só existem junto aos provedores e estão sob seu controle. Os clientes devem identificar claramente as responsabilidades dos provedores com relação à investigação forense. Os SLOs podem incluir fontes de evidências como registros do perímetro da rede em nuvem, servidores DNS, monitor de máquinas virtuais, APIs, sistema operacional host, captura de rede, e portal de faturamento e gestão.

Investigar possíveis violações em ambientes de nuvem implica outros desafios. Por exemplo, instâncias de VM comprometidas podem ser desativadas antes que qualquer pessoa esteja ciente de que ocorreu uma violação. Pode ser quase impossível investigar adequadamente uma violação quando a fonte da violação não estiver mais em uso ou sequer existir.

¹⁷ Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V4.0 (Cloud Security Alliance, 2017). <https://cloudsecurityalliance.org/download/security-guidance-v4>.

¹⁸ Cloud Security Alliance, Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing (Cloud Security Alliance, June 2013). <https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf>.

6.4.3 Notificação de violação

Os clientes devem exigir contratualmente de seus provedores a notificação de violação de dados em linguagem clara e inequívoca, levando em consideração a necessidade de cumprir as leis regulatórias/sobre violações nacionais e globais, a privacidade de dados, a gestão de incidentes de segurança e os requisitos de notificação de violação.

As categorias de incidentes de dados e de segurança devem ser priorizadas com prazos esperados para notificação, dependendo do tipo de incidente e dos requisitos estabelecidos pelo cliente, e quando necessário, devem incluir:

- Responsabilidades e obrigações definidas de resposta de notificação de violação
- Informações de contato dos clientes (por exemplo, e-mail para incidentes de menor prioridade ou número de telefone para resposta a incidentes 24 horas por dia, 7 dias por semana, para incidentes de alta prioridade)
- Direitos de envolver as equipes forenses do cliente ou da bandeira do cartão na investigação de um incidente ou de uma violação

Da mesma forma, os provedores talvez queiram exigir contratualmente que seus clientes os informem sobre qualquer comprometimento suspeito ou real, por exemplo, violação de credenciais de autenticação ou vulnerabilidades de serviço identificadas. Quando uma notificação de incidente é recebida pelo provedor ou pelo cliente, é responsabilidade de tal parte seguir o plano de resposta a incidentes implementado (de acordo com o Requisito 12.10 do PCI DSS). Além disso, os provedores são obrigados a realizar revisões pelo menos trimestralmente para confirmar que os funcionários estão seguindo os processos estabelecidos para responder a alertas de segurança (Requisito 12.11 do PCI DSS).

6.5 Gestão de vulnerabilidades

Testes proativos, identificação e mitigação de vulnerabilidades são parte importante para se alcançar e manter a conformidade com o PCI DSS para ambientes que utilizam serviços e sistemas em nuvem. No PCI DSS, são seis áreas distintas de gestão de vulnerabilidades: testes de vulnerabilidades de aplicativos da Web (Requisito 6.6 do PCI DSS), varredura de vulnerabilidades da rede interna (Requisito 11.2.1 do PCI DSS), varredura de vulnerabilidades da rede externa (Requisito 11.2.2 do PCI DSS), testes de penetração externa (Requisito 11.3.1 do PCI DSS), testes de penetração interna (Requisito 11.3.2 do PCI DSS) e testes de segmentação (Requisito 11.3.4 do PCI DSS).

O escopo é um elemento crítico da gestão de vulnerabilidades. Os clientes precisam garantir que identifiquem adequadamente todos os sistemas e serviços dentro do escopo, incluindo aqueles fornecidos pelo provedor, aqueles pelos quais o cliente e o provedor tenham responsabilidade compartilhada e aqueles que se referem exclusivamente ao cliente (por exemplo, sistemas ou aplicativos no local, em nuvem privada ou híbridos, ou sistemas que o cliente mantém). O teste de penetração é usado para confirmar os controles de segmentação destinados a restringir o escopo e para identificar proativamente vulnerabilidades que poderiam ser exploradas para permitir que um invasor violasse esses limites.

Testar vulnerabilidades na nuvem também requer uma compreensão aprofundada do modelo de implantação em nuvem para determinar a responsabilidade quando se trata de realizar o exercício de teste apropriado. É fundamental entender os aspectos do ambiente que serão testados pelo provedor e aqueles que precisarão ser testados pelo cliente. Não basta identificar a responsabilidade pelo sistema físico, pois cada entidade pode ter responsabilidade distinta ou compartilhada em relação aos aspectos de um sistema físico (por exemplo, hardware físico, hipervisor, sistema operacional convidado, aplicativo, configuração). Essas responsabilidades variarão dependendo do modelo de entrega do serviço em nuvem (ou seja, IaaS, SaaS, PaaS) ou outra divisão de controle.

Quando houver responsabilidade compartilhada pelas atividades de teste de vulnerabilidades, o cliente e o provedor devem cooperar para garantir que esses testes sejam realizados e que as vulnerabilidades sejam resolvidas. Em última análise, é responsabilidade do cliente fornecer evidências de que todos os testes necessários tenham sido realizados.

O PCI Security Standards Council publicou o Suplemento de informações *Orientação para testes de penetração*, com o objetivo de promover mais compreensão sobre os requisitos, as metodologias e os princípios dos testes de penetração, conforme aplicável ao ambiente do PCI DSS.¹⁹

6.5.1 Testes de vulnerabilidades dos aplicativos da Web

Todos os aplicativos da Web voltados para o público devem estar protegidos, seja pela implantação de uma solução técnica automatizada que detecta e previne ataques baseados na Web ou pela realização de testes de segurança de vulnerabilidades de aplicativos de acordo com o Requisito 6.6 do PCI DSS. Se um provedor estiver fornecendo um aplicativo da Web (por exemplo, um aplicativo SaaS) que armazena, processa, transmite ou afeta a segurança dos dados do titular do cartão, o aplicativo deverá ser protegido por um firewall de aplicativo da Web (ou solução semelhante) ou testado pelo provedor, e isso deve ser refletido no AOC e na matriz de responsabilidades do provedor. Os provedores que expõem APIs para seus clientes também devem realizar testes e emitir relatórios sobre essas APIs.

Para aplicativos que são fornecidos pelo cliente (por exemplo, um microsserviço sendo executado em um serviço PaaS ou IaaS), é responsabilidade do cliente executar testes de segurança de vulnerabilidades de aplicativos da Web como parte de seu programa de conformidade do PCI. Os provedores devem reconhecer esse requisito e apoiar essas atividades de teste exigidas (por exemplo, ao apoiar a capacidade de desativar controles que impediriam testes controlados, ao apoiar aplicativos que possam executar essas operações ou ao oferecer um serviço para desempenhar esses serviços).

¹⁹ Orientação para testes de penetração Grupo de interesse especial e PCI Security Standards Council, Orientação para testes de penetração, (PCI SSC, setembro de 2017), https://www.pcisecuritystandards.org/documents/Participation-Testing-Guidance-v1_1.pdf.

6.5.2 Varredura de vulnerabilidades da rede

O cliente é responsável por garantir que as varreduras de vulnerabilidades da rede (Requisito 11.2 do PCI DSS) sejam realizadas de forma compatível, embora esta exigência possa ser atendida pelo provedor ou por outro serviço qualificado de terceiros. A entidade que mantém os sistemas físicos, dispositivos de rede, sistemas operacionais e aplicativos em rede geralmente seria responsável por desempenhar as varreduras necessárias para garantir que esses serviços estejam livres de vulnerabilidades conhecidas. Por exemplo, um provedor que presta um serviço SaaS geralmente seria responsável por desempenhar essas varreduras e abordar as vulnerabilidades encontradas nos sistemas operacionais e aplicativos que ele mantém. Nos modelos de entrega PaaS e IaaS, poderá haver responsabilidade compartilhada, pois cada entidade deve fazer a varredura dos dispositivos, sistemas operacionais convidados, hipervisores e aplicativos pelos quais é responsável.

6.5.2.1 Varredura de vulnerabilidades da rede interna

Todos os sistemas ou serviços conectados no CDE devem ser varridos em busca de vulnerabilidades da rede interna trimestralmente ou quando alterações significativas tiverem sido feitas nas regras de firewall ou na topologia da rede (por exemplo, redes virtuais, grupos de segurança, listas de controle de acesso (access control lists, ACLs)). Essa operação pode exigir o início de uma VM ou de um aplicativo dentro da rede para desempenhar o serviço de varredura ou o provedor talvez deseje oferecer um serviço de varredura qualificado para apoiar essas atividades.

6.5.2.2 Varredura de vulnerabilidades da rede externa

Todos os IPs externos endereçáveis publicamente ao CDE devem ser varridos em busca de vulnerabilidades por um provedor de varredura autorizado (Authorized Scanning Vendor, ASV) trimestralmente ou quando alterações significativas tiverem sido feitas nas regras de firewall ou na topologia da rede (por exemplo, redes virtuais, grupos de segurança, ACLs). Onde a rota das redes virtuais atravessar o espaço IP público, esses endereços IP deverão ser incluídos nesse requisito, mesmo que esses IPs sejam considerados privados devido aos controles da rede (por exemplo, emparelhamento).

6.5.3 Testes de penetração

Para atender ao propósito do Requisito 11.3 do PCI DSS, os testes de penetração do CDE devem incluir tanto a infraestrutura (rede virtual, grupo de segurança, ACL, sistema operacional convidado e acima) quanto testes de penetração de aplicativos quando aplicável.

6.5.3.1 Teste de penetração externa

As atividades de testes de penetração a partir de uma fonte externa devem ser iniciadas em toda a rede pública não confiável. Se desejado, eles podem ser iniciados a partir de instâncias virtuais hospedadas pelo mesmo provedor, mas esses sistemas devem atravessar o espaço IP roteado publicamente e não ter acesso direto ao CDE para garantir a simulação de um ataque externo.

6.5.3.2 Teste de penetração interna

O teste de penetração a partir da rede interna deve ser realizado a partir de segmentos de rede que tenham acesso suficiente a sistemas críticos. Esse teste deve simular um ataque por parte de uma entidade contra a infraestrutura interna (quando permitido pelo provedor), em que o invasor já obteve acesso à rede virtual interna. Dependendo da arquitetura da rede virtual, bem como dos controles de segurança implementados, o teste de penetração interna poderia ser realizado a partir do CDE ou de outros segmentos de rede virtual interna (por exemplo, VLAN de gerenciamento).

6.5.3.3 Testes de segmentação

A segmentação de testes (Requisito 11.3.4 do PCI DSS) na nuvem pode ser desafiadora, já que vários controles de segmentação podem ser usados para isolar sistemas, incluindo ACLs, firewalls, redes definidas por software (Software Defined Networking, SDN) e roteamento de rede. Para limitar o escopo, os testes de penetração devem ser realizados para testar a adequação desses controles a fim de confirmar que os controles estão operacionais e são eficazes. Os testes de validação devem incluir testes entre VMs/instâncias, entre aplicativos/microserviços hospedados em redes virtuais separadas.

O provedor deve realizar testes de penetração como parte de sua própria avaliação do PCI DSS para demonstrar a separação das redes dos clientes a fim de ajudar os clientes a atender a esse requisito. Esses devem incluir testes entre nós de gerenciamento do provedor e sistemas dos clientes, e entre clientes em infraestrutura compartilhada. Os testes devem ser usados para verificar se há controles de rede restritivos adequados em vigor para separar os ambientes (por exemplo, avaliar a eficácia dos controles de rede restritos implementados nos grupos de segurança/firewall ou ACLs).

6.5.4 *Notificação de testes*

Considerando a natureza dinâmica da nuvem, os ambientes compartilhados nos quais os testes de gestão de vulnerabilidades devem ser realizados e a relação colaborativa dos provedores e clientes, pode ser necessário fornecer aviso e obter permissão prévia antes de tentar desempenhar determinadas atividades de teste. A notificação pode incluir datas de testes antecipadas, tipos de testes e detalhes como o(s) intervalo(s) de endereços IP afetado(s). Também é importante para o cliente entender quais atividades de teste são permitidas pelo provedor e garantir que tais atividades não prejudiquem outros clientes no ambiente. Tais restrições devem ser detalhadas nos contratos de serviço, nos termos de serviço ou na política de uso aceitável.

Apêndice A: exemplo de responsabilidades do PCI DSS para diferentes categorias de serviço em nuvem

Este Apêndice expande a Tabela 2 (na Seção 4) e fornece exemplos de como as responsabilidades referentes aos requisitos do PCI DSS poderão ser compartilhadas entre clientes e provedores em algumas das várias categorias de serviços em nuvem. Obviamente, haverá exceções e variações em cada serviço individual e esta tabela é fornecida como uma diretriz para os clientes e provedores com o objetivo de ajudar a planejar discussões e negociações.

As descrições nessa tabela se destinam a refletir as responsabilidades do provedor com relação aos serviços que prestam e não consideram as responsabilidades do provedor, uma vez que sua infraestrutura interna e suas operações não estão diretamente envolvidas na prestação de serviços aos seus clientes. Da mesma forma, as responsabilidades do cliente não incluem consideração quanto aos sistemas do cliente usados para acessar o serviço em nuvem ou para quaisquer sistemas do cliente dentro do escopo do PCI DSS que estejam fora do serviço em nuvem.

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 1: <i>Instalar e manter uma configuração de firewall para proteger os dados do titular do cartão.</i>	<p>IaaS: normalmente, a segurança da rede é uma responsabilidade compartilhada: o cliente é responsável por proteger as redes dentro e entre seus próprios ambientes, enquanto o provedor fornece segurança de rede no perímetro da nuvem e entre seus clientes. O provedor gerencia firewalls na rede gerenciada pelo provedor e em quaisquer firewalls de infraestrutura não visíveis para o cliente. Quaisquer firewalls acima da camada de infraestrutura poderão ser de responsabilidade do cliente. Os firewalls gerenciados pelo provedor também poderiam ser compartilhados por vários clientes.</p> <p>PaaS: firewalls acima da camada de infraestrutura poderão ser de responsabilidade do cliente ou do provedor. O cliente poderia ser diretamente responsável pela implementação e gerenciamento de firewalls na plataforma fornecida ou poderá definir configurações de firewall, que, em seguida, o provedor implementa para o ambiente do cliente. Os firewalls gerenciados pelo provedor também poderiam ser compartilhados com outros clientes.</p> <p>SaaS: a rede é de propriedade integral do provedor e gerenciada por ele, e, conseqüentemente, todas as funções de firewall costumam ser gerenciadas pelo provedor.</p> <p>Em todas as situações, talvez o cliente ainda tenha de definir, aprovar e revisar periodicamente os serviços, os protocolos e as portas permitidas em seu ambiente, mesmo que o provedor estiver gerenciando os firewalls em questão.</p>	Cliente e provedor	Cliente e provedor	Provedor

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 2: <i>não usar padrões disponibilizados pelo provedor para senhas do sistema e outros parâmetros de segurança.</i>	<p>IaaS: a configuração segura do sistema operacional e dos aplicativos geralmente é responsabilidade do cliente, enquanto a configuração segura dos dispositivos subjacentes é responsabilidade do provedor. Também pode haver dispositivos virtuais cuja manutenção é responsabilidade do cliente.</p> <p>PaaS: o sistema operacional frequentemente é controlado pelo provedor, mas alguns serviços podem incluir um nível de acesso do cliente ao sistema operacional – ambas as partes precisarão esclarecer qual entidade está aplicando a configuração segura e fortalecendo no nível do sistema operacional. Aplicativos e softwares acima do sistema operacional provavelmente são controlados pelo cliente. A configuração segura dos dispositivos de rede será gerenciada pelo provedor.</p> <p>SaaS: o provedor costuma gerenciar a configuração e o fortalecimento de todos os dispositivos sistemas operacionais e aplicativos.</p>	Cliente e provedor	Cliente e provedor	Provedor
Requisito 3: <i>proteger os dados armazenados do titular do cartão.</i>	<p>IaaS e PaaS: o cliente geralmente é responsável pela maneira em que as informações são protegidas (como o uso de mecanismos de criptografia) e em que formato – por exemplo, arquivos simples, entradas do banco de dados etc. Os locais físicos dos armazenamentos das informações podem ser desconhecidos ao cliente, e os locais de armazenamento talvez precisem ser identificados. A retenção de dados é definida pelo cliente; no entanto, o provedor controla as áreas de armazenamento reais. O uso de controles para evitar retenção não intencional ou adicional (por exemplo, via snapshots, backups etc.) também precisa ser considerado.</p> <p>SaaS: os dados armazenados do titular do cartão normalmente são controlados e gerenciados pelo provedor como parte do serviço predefinido. O provedor também pode definir os períodos de retenção. Os clientes podem ter muito pouco ou nenhum controle sobre como ou onde seus dados, incluindo CHD, são armazenados.</p>	Cliente e provedor	Cliente e provedor	Provedor

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 4: <i>codificar a transmissão dos dados do titular do cartão em redes abertas e públicas.</i>	<p>IaaS e PaaS: os mecanismos de transmissão costumam ser controlados pelo cliente, enquanto a tecnologia subjacente é gerenciada pelo provedor; entretanto, isso dependerá das tecnologias em uso. Os controles para evitar a transmissão não intencional de dados fora do ambiente do cliente geralmente são mantidos pelo provedor, dependendo do serviço específico. O cliente deve estar ciente de como os dados são transmitidos entre os componentes para garantir que os dados sejam criptografados para todas as transmissões em canais não privados. Isso pode incluir transmissões dentro do próprio ambiente do cliente (por exemplo, entre VMs do cliente).</p> <p>SaaS: o provedor retém o controle total sobre os mecanismos de transmissão. O cliente tem pouco ou nenhum controle sobre como ou onde os dados são transmitidos dentro do ambiente de nuvem. O cliente é responsável por garantir que os dados “clear-text” não sejam passados ao provedor para transmissão para redes públicas ou ambientes não confiáveis (como outros clientes em nuvem).</p>	Cliente	Cliente e provedor	Provedor
Requisito 5: <i>proteger todos os sistemas contra malware e atualizar regularmente os programas ou softwares antivírus.</i>	<p>IaaS: a proteção do sistema operacional e das VMs do cliente costuma ser responsabilidade do cliente. As atualizações antivírus se aplicam ao sistema operacional host, bem como a quaisquer VMs no ambiente do cliente executando seus próprios sistemas operacionais. Também pode haver dispositivos virtuais cuja atualização é responsabilidade do cliente. A proteção antimalware para dispositivos/infraestrutura subjacentes permanece sendo responsabilidade do provedor.</p> <p>É importante confirmar que a solução antivírus selecionada usada pelo cliente é compatível com a infraestrutura subjacente gerenciada pelo provedor.</p> <p>PaaS: a proteção contra malware geralmente é gerenciada por quem controla o sistema operacional; alguns serviços PaaS incluem a responsabilidade do cliente pela manutenção do sistema operacional. As atualizações antivírus serão aplicadas ao sistema operacional subjacente, bem como a quaisquer VMs no ambiente do cliente executando seu próprio sistema operacional.</p> <p>SaaS: o provedor normalmente gerencia a segurança e o antivírus para o ambiente.</p>	Cliente	Cliente e provedor	Provedor

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 6: Desenvolver e manter sistemas e aplicativos seguros.	IaaS: A correção e a manutenção do sistema operacional e dos aplicativos geralmente são responsabilidade do cliente, enquanto a correção e a manutenção dos dispositivos subjacentes permanecem sendo responsabilidade do provedor. Também pode haver dispositivos virtuais cuja manutenção é responsabilidade do cliente. A codificação segura normalmente é responsabilidade do cliente (ele pode usar seus próprios aplicativos ou escolher aplicativos comerciais seguros).			
	PaaS: a correção e a manutenção dos dispositivos subjacentes permanecem sendo responsabilidade do provedor. A correção e a manutenção do sistema operacional também podem ser controladas pelo provedor; entretanto, alguns serviços PaaS incluem a responsabilidade do cliente pela manutenção do sistema operacional: as entidades precisarão determinar qual parte é responsável por aplicar patches/atualizações. Se o provedor fornecer patches, o cliente deve verificar se os patches são implantados em tempo hábil. A correção de aplicativos normalmente é gerenciada pelo cliente, dependendo do serviço e dos acordos. A codificação segura dos aplicativos é responsabilidade de quem desenvolve/controla os aplicativos, que pode ser o cliente ou o provedor, e pode variar para diferentes aplicativos.	Cliente e Provedor	Cliente e Provedor	Cliente e Provedor
	SaaS: o cliente pode controlar ou gerenciar as APIs, ou pode compartilhar a responsabilidade com o provedor. O provedor normalmente gerencia patches e atualizações de todos os dispositivos, sistemas operacionais e aplicativos, e também é responsável pela codificação segura do software; no entanto, o cliente deve verificar se os patches são implantados em tempo hábil.			

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 7: restringir o acesso aos dados do titular do cartão de acordo com a necessidade de divulgação dos negócios.	<p>IaaS e PaaS: geralmente, o cliente é responsável por definir o acesso aos seus arquivos de dados. A localização física dos armazenamentos de informações pode ser desconhecida ao cliente, e talvez precise ser identificada. O provedor controla as áreas de armazenamento físico e os controles de acesso gerenciados pelo provedor frequentemente são cumulativos aos controles definidos pelo cliente. O uso de controles para impedir o acesso não intencional aos dados (por exemplo, a dados capturados via snapshots, backups etc.) também deve ser considerado.</p> <p>SaaS: o cliente define as necessidades de acesso aos dados para seu próprio pessoal; no entanto, o acesso aos dados é controlado, em última análise, pelo provedor.</p>	Cliente e Provedor	Cliente e Provedor	Cliente e Provedor
Requisito 8: identificar e autenticar o acesso aos componentes do sistema.	<p>IaaS e PaaS: o cliente é responsável por garantir que todas as contas sob seu controle usem IDs exclusivas e autenticação forte. O provedor é responsável por garantir que a autenticação forte seja usada para a infraestrutura subjacente. Em comparação com a categoria de serviço em nuvem IaaS, o provedor retém direitos de acesso administrativo significativos em categorias de serviço em nuvem SaaS e PaaS.</p>	Cliente e Provedor	Cliente e Provedor	Cliente e Provedor
	<p>SaaS: o provedor detém o controle final das contas em todos os níveis. Dependendo do serviço específico, o cliente pode ter a capacidade de criar contas de nível de usuário dentro do aplicativo ou serviço, ou poderá receber a atribuição de contas de usuário que o provedor mantém em seu nome. O cliente é responsável por garantir que todas as contas que ele usa tenham senhas fortes.</p>			
Requisito 9: restringir o acesso físico aos dados do titular do cartão.	<p>Todas as categorias de serviço em nuvem: o acesso físico ao CHD geralmente é gerenciado pelo provedor para todas as categorias de serviço em nuvem. O cliente raramente tem acesso físico aos sistemas de nuvem; e o provedor pode não permitir visitas no local ou auditorias do cliente. Isso dependerá do provedor específico, bem como da distribuição de dados em diferentes locais; os clientes podem não saber qual local armazena seus dados.</p>	Provedor	Provedor	Provedor

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 10: rastrear e monitorar todo o acesso aos recursos da rede e aos dados do titular do cartão.	<p>IaaS e PaaS: o provedor normalmente gerencia o monitoramento e o registro dos dispositivos e da infraestrutura subjacentes, incluindo hipervisores, enquanto o cliente é responsável por monitorar e registrar seus próprios ambientes virtuais. A capacidade de associar vários arquivos de registro a fim de reconstruir eventos pode exigir uma correlação entre registros controlados pelo cliente e aqueles controlados pelo provedor.</p> <p>Algumas atividades de monitoramento podem ser incorporadas ao acordo de serviço para que o provedor gerencie em nome dos clientes. Os detalhes sobre quais dados serão capturados e o que será disponibilizado para o cliente precisam ser definidos.</p> <p>SaaS: o cliente normalmente conta com o provedor para todo o monitoramento e o registro, mas pode ter registro limitado no nível do aplicativo, como logon/logoff de usuário, gerenciamento de contas e emissão de relatórios básicos.</p>	Cliente e Provedor	Cliente e Provedor	Cliente e Provedor
Requisito 11: testar regularmente os sistemas e processos de segurança.	<p>IaaS e PaaS: os testes geralmente são gerenciados por quem tem controle do aspecto específico do ambiente. No entanto, os provedores podem proibir testes do cliente, caso em que os clientes podem precisar contar com o provedor. Se o provedor estiver realizando varreduras, o cliente precisa verificar quais instâncias/VMs estão cobertas. Sistemas de detecção de invasão (Intrusion Detection Systems, IDS)/sistemas de prevenção de invasão (Intrusion Prevention Systems, IPS) não podem ser fornecidos pelo provedor. Geralmente, o cliente pode usar o monitoramento de integridade de arquivos (File Integrity Monitoring, FIM) para monitorar seus próprios ambientes virtuais (incluindo dados, aplicativos e registros), enquanto o monitoramento dos arquivos do sistema/do dispositivo é gerenciado pelo provedor.</p> <p>SaaS: o cliente não tem visibilidade ou permissão para realizar varreduras e costuma depender do provedor para todas as varreduras, testes e monitoramento.</p>	Cliente e provedor	Cliente e provedor	Provedor

Requisitos do PCI DSS	Considerações comuns	Exemplo de atribuição de responsabilidade para a gestão de controles		
		IaaS	PaaS	SaaS
Requisito 12: manter uma política que aborde a segurança das informações para todas as equipes.	Todas as categorias de serviço em nuvem: embora o provedor e o cliente possam definir procedimentos acordados (por exemplo, no SLA), cada parte mantém suas próprias políticas de segurança e procedimentos internos. Funções e responsabilidades definidas, treinamento e requisitos de segurança de pessoal são responsabilidade de cada parte para seus respectivos funcionários. Os clientes devem garantir que as políticas e os procedimentos do provedor sejam apropriados para as necessidades de risco e de segurança do cliente. Em especial, a resposta a incidentes requer conscientização e coordenação entre ambas as partes.	Cliente e Provedor	Cliente e Provedor	Cliente e Provedor
Apêndice A1: requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada	Os requisitos para provedores de hospedagem compartilhada para assegurar a separação entre os clientes se aplicam a serviços de nuvem prestados por terceiros.	Provedor	Provedor	Provedor

Apêndice B: inventário de amostras

Este apêndice fornece um inventário de exemplos para componentes usados em ambientes de nuvem. O uso de um inventário pode ajudar a identificar os tipos de componentes envolvidos na entrega do serviço e a responsabilidade por protegê-los. Este exemplo não se destina a ser aplicável a qualquer situação específica, mas, sim, a fornecer um ponto de partida para discussões de determinação do escopo entre clientes e provedores.

Ao preparar um inventário, considere o seguinte:

- O tipo de informação coletada deve ser relevante para as necessidades comerciais do cliente, bem como para o provedor.
- O nível de detalhe coletado deve ser apropriado para ambas as partes obterem uma compreensão clara dos componentes envolvidos, do seu uso e de quem os gerencia/protege.

Tipo/camada	Descrição/finalidade do componente	Tipo de componente	Número de componentes	Notas de implementação	Responsabilidade pela segurança do componente
<i>Observação: as camadas reais variarão dependendo da estrutura das ofertas de serviço do provedor.</i>	<i>Por exemplo: firewall, sistema operacional, aplicativo, servidor Web, hipervisor, roteador, banco de dados etc.</i>	<i>Por exemplo: o componente é físico, lógico ou virtual? Estático ou dinâmico?</i>	<i>Número de componentes usados em relação ao serviço do cliente</i>	<i>Uso definido, localização etc., conforme aplicável</i>	<i>Por exemplo: Apenas provedor, apenas cliente, ou compartilhado</i>
Dados					
Interfaces – APIs/GUIs					
Aplicativos					
Pilha de programação					
Sistemas operacionais					
Máquinas virtuais					
Rede virtual					

Tipo/camada	Descrição/finalidade do componente	Tipo de componente	Número de componentes	Notas de implementação	Responsabilidade pela segurança do componente
<i>Observação: as camadas reais variarão dependendo da estrutura das ofertas de serviço do provedor.</i>	<i>Por exemplo: firewall, sistema operacional, aplicativo, servidor Web, hipervisor, roteador, banco de dados etc.</i>	<i>Por exemplo: o componente é físico, lógico ou virtual? Estático ou dinâmico?</i>	<i>Número de componentes usados em relação ao serviço do cliente</i>	<i>Uso definido, localização etc., conforme aplicável</i>	<i>Por exemplo: Apenas provedor, apenas cliente, ou compartilhado</i>
Hipervisores					
Contêineres					
Processamento/Memória					
Armazenamento de dados					
Dispositivos de rede					
Servidores físicos					
Instalações físicas					

Observação: o objetivo é fornecer apenas um exemplo geral. Pode ser necessário reorganizar as diferentes camadas de tecnologia ou definir características adicionais dos componentes, conforme aplicável a um ambiente específico. Além disso, as entidades podem querer identificar as responsabilidades para cada componente do sistema com mais detalhes do que o fornecido aqui.

Apêndice C: exemplo da matriz de gestão de responsabilidades do PCI DSS

Uma matriz de responsabilidades do PCI DSS pode ajudar a esclarecer e confirmar como as responsabilidades por manter os requisitos do PCI DSS são compartilhadas entre o cliente e o provedor. As responsabilidades sempre devem ser definidas em acordos por escrito.

A tabela abaixo, que é um exemplo de um modelo que pode ser usado pelos provedores e clientes para comunicar as responsabilidades e considerações para cada requisito do PCI DSS, inclui:

- O provedor realiza/gerencia/mantém o controle exigido?
- Como o controle é implementado e quais são os processos de apoio, por exemplo, o processo de atualizações de patches incluiria detalhes de testes, programação, aprovações etc.?
- Quais camadas da arquitetura de nuvem são cobertas pelo provedor em relação ao requisito? Quais camadas da arquitetura não são cobertas pelo provedor e são especificamente responsabilidade do cliente?
- Como o provedor fornecerá garantia contínua ou evidência ao cliente de que os controles são atendidos, por exemplo, relatórios periódicos, notificações em tempo real, resultados de testes etc.?

Requisito do PCI DSS	Responsabilidade (Apenas provedor, apenas cliente ou compartilhada)	Cobertura específica/escopo do cliente Responsabilidade	Cobertura específica/escopo da responsabilidade do provedor	Como e quando o provedor fornecerá evidências de Conformidade com o cliente
1.1 Definir os padrões de configuração do firewall e do roteador que incluam o seguinte:				
1.1.1 Um processo formal para aprovar e testar todas as conexões de rede e alterações às configurações do firewall e do roteador				
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 quaisquer redes wireless				

Requisito do PCI DSS	Responsabilidade (Apenas provedor, apenas cliente ou compartilhada)	Cobertura específica/escopo do cliente Responsabilidade	Cobertura específica/escopo da responsabilidade do provedor	Como e quando o provedor fornecerá evidências de Conformidade com o cliente
1.1.3 Diagrama atual que mostra todos os fluxos de dados do titular do cartão em todos os sistemas e redes				
1.1.4 Requisitos para um firewall em cada conexão da internet e entre qualquer zona desmilitarizada (demilitarized zone, DMZ) e a zona de rede interna				
1.1.5 Descrição de grupos, funções e responsabilidades quanto ao gerenciamento lógico dos componentes da rede				
...e assim por diante.				

Observação: o objetivo é fornecer apenas um exemplo como ponto de partida para discussões entre clientes e provedores. Não se destina a constituir um requisito ou uma extensão das responsabilidades de conformidade do PCI DSS. No entanto, pode fornecer uma ferramenta útil para ajudar a esclarecer as responsabilidades em acordos entre clientes e provedores.

Apêndice D: considerações sobre implementação do PCI DSS

As perguntas neste apêndice são sugestões para ajudar a iniciar conversas entre clientes e provedores a fim de compreender as características de um ambiente de nuvem específico, o que, por sua vez, pode ajudar a determinar se e como os requisitos do PCI DSS podem ser atendidos nesse ambiente. Essas perguntas isoladas não determinarão se os requisitos aplicáveis do PCI DSS podem ou não ser cumpridos; entretanto, elas podem ser úteis para perguntas diretamente relacionadas a requisitos específicos do PCI DSS.

As informações nesta tabela incorporam orientação das seguintes fontes:

- Questionário de iniciativa de avaliações consensuais da CSA
- Requisitos de garantia de informações da ENISA

Consulte também as Diretrizes de virtualização do PCI DSS para outras considerações do PCI DSS sobre tecnologias de virtualização.

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Construir e manter uma rede segura</p> <p><i>Requisito 1: instalar e manter uma configuração de firewall para proteger os dados do titular do cartão.</i></p> <p><i>Requisito 2: não usar padrões disponibilizados pelo provedor para senhas do sistema e outros parâmetros de segurança.</i></p>	<ul style="list-style-type: none"> ▪ Como a separação entre os locatários é garantida? ▪ Como os limites são fiscalizados entre redes confiáveis (internas ao cliente) e redes não confiáveis (como redes do provedor, redes de outros clientes ou redes voltadas para o público)? ▪ São usados firewalls físicos ou virtuais? ▪ Quem gerencia e audita as configurações de firewall? ▪ Como as alterações nas configurações de firewall e rede são rastreadas e gerenciadas? ▪ Quais tecnologias são usadas na prestação do serviço em nuvem, por exemplo, hardware, software, tecnologias virtuais? <ul style="list-style-type: none"> ○ Existe uma lista atual de todos os componentes de hardware e software no ambiente? ○ Os componentes reais usados por um cliente específico podem ser identificados? ▪ Como os padrões de configuração são garantidos em diferentes componentes da infraestrutura? <ul style="list-style-type: none"> ○ As interfaces API são padronizadas? ○ Qual é o processo para o provisionamento de novos componentes? ○ As imagens virtuais são fortalecidas antes de serem habilitadas? ○ As imagens fortalecidas são protegidas contra acesso não autorizado? ▪ Como os sistemas com classificações de alta segurança são segregados de sistemas com classificações de baixa segurança? ▪ Como os recursos compartilhados (como processamento, memória e armazenamento) são gerenciados para garantir que não possam ser manipulados, por exemplo ao sobrecarregar, para obter acesso a outros ambientes ou dados do cliente?

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Proteger os dados do titular do cartão</p> <p><i>Requisito 3: proteger os dados armazenados do titular do cartão.</i></p> <p><i>Requisito 4: codificar a transmissão dos dados do titular do cartão em redes abertas e públicas.</i></p>	<ul style="list-style-type: none"> ▪ Onde estão os locais de armazenamento de dados conhecidos? Onde estão localizados os data centers? ▪ Quais jurisdições legais se aplicam aos dados do cliente? ▪ O provedor tem algum requisito comercial, legal ou regulatório que possa afetar a retenção dos dados do cliente? ▪ Como o acesso aos dados do cliente é restrito apenas aos usuários e aplicativos do cliente? ▪ Como as imagens de VM, snapshots e backups são gerenciados para prevenir a captura desnecessária de dados confidenciais? ▪ Como os dados são excluídos com segurança da memória e das imagens armazenadas? Há dados residuais em VMs encerradas? ▪ Se chaves criptográficas forem fornecidas pelo provedor, chaves exclusivas são geradas para cada cliente? ▪ Onde os processos de criptografia/descriptografia estão sendo realizados? Quem controla cada processo? ▪ Onde as chaves criptográficas são armazenadas e quem controla as chaves? As chaves de criptografia de dados são armazenadas e gerenciadas separadamente dos dados que protegem? ▪ Onde os dados criptografados são armazenados e quem tem acesso às chaves e aos dados criptografados? ▪ Como a segurança e o acesso são definidos para os recursos virtualizados usados para a geração de chaves criptográficas? ▪ Qual processo é seguido em caso de suspeita de comprometimento das chaves? ▪ Todos os dados do cliente são removidos com segurança de todos os sistemas do provedor após o encerramento do acordo? ▪ Como as comunicações são protegidas entre o cliente e outros ambientes? Como as comunicações são protegidas dentro da própria nuvem? ▪ As APIs são configuradas para aplicar criptografia e autenticação fortes? ▪ A autenticação mútua é implementada entre os sistemas do provedor e do cliente?

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Manter um programa de gestão de vulnerabilidades</p> <p><i>Requisito 5: proteger todos os sistemas contra malware e atualizar regularmente programas ou software antivírus.</i></p> <p><i>Requisito 6: desenvolver e manter sistemas e aplicativos seguros.</i></p>	<ul style="list-style-type: none"> ▪ As VMs são protegidas de dentro da VM ou do hipervisor? ▪ Como é assegurado que as imagens de VM (incluindo VMs inativas e replicadas) tenham antimalware e patches atualizados antes de estarem habilitados para uso? ▪ Como os patches são gerenciados (por exemplo, priorizados, testados, aprovados e implementados) para os sistemas subjacentes do provedor e ambientes provisionados do cliente? <ul style="list-style-type: none"> ○ Qual é o processo para cada camada do serviço em nuvem – por exemplo, dispositivos de rede física, firmware, sistemas operacionais host, hipervisores, componentes virtualizados (incluindo VMs, dispositivos de rede virtual), aplicativos etc.? ▪ Como as APIs e os serviços da Web são protegidos contra vulnerabilidades? ▪ Interfaces e linguagens de codificação padronizadas são usadas? ▪ Como é feita a prevenção da migração inadvertida de sistemas de desenvolvimento/teste e dados para ambientes de produção e vice-versa (por exemplo, através de mecanismos de replicação virtual, imagem ou snapshot)?

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Implementar medidas rigorosas de controle de acesso</p> <p><i>Requisito 7: restringir o acesso aos dados do titular do cartão de acordo com a necessidade de divulgação dos negócios.</i></p> <p><i>Requisito 8: identificar e autenticar o acesso aos componentes do sistema.</i></p> <p><i>Requisito 9: restringir o acesso físico aos dados do titular do cartão.</i></p>	<ul style="list-style-type: none"> ▪ Como a autenticação do usuário é aplicada em diferentes níveis? ▪ Como as camadas de controles de acesso são gerenciadas para garantir que o acesso agregado não seja mais do que o pretendido? ▪ Que pessoal do provedor pode acessar dados do cliente? ▪ Como são revisadas e monitoradas as atribuições de privilégios do provedor? ▪ Como é mantida a separação de tarefas (por exemplo, entre funções administrativas e de auditoria)? <ul style="list-style-type: none"> ○ O acesso administrativo a sistemas ou ao hipervisor é separado do acesso às VMs e aos armazenamentos de dados do cliente? ○ São usadas credenciais separadas para diferentes funções de segurança? ▪ Como são determinados os privilégios mínimos e a necessidade de saber para o pessoal do provedor? ▪ Como as credenciais são desprovisionadas? <ul style="list-style-type: none"> ○ O desprovisionamento se aplica a todos os locais distribuídos geograficamente? ○ As credenciais desprovisionadas poderiam ser retidas em imagens offline? ▪ O acesso remoto para o pessoal do provedor é permitido a partir de redes não confiáveis? ▪ Existem controles implementados para prevenir a captura de senhas na memória ativa e para garantir que imagens virtualizadas não contenham credenciais de autenticação? ▪ É necessária a autenticação de dois fatores para o acesso do cliente? ▪ O provedor usa senhas compartilhadas (por exemplo, para manutenção)? ▪ O provedor mantém propriedade e controle diretos sobre todos os sistemas e instalações de armazenamento de dados? ▪ Quem tem acesso físico aos data centers e sistemas? ▪ Como os sistemas de armazenamento de dados são protegidos contra acesso físico ou direto ao console? ▪ Como os backups de VMs e dados são protegidos? ▪ Como a mídia física é inventariada, protegida, monitorada e rastreada? ▪ A mídia é reutilizada? Como os dados são removidos permanentemente da mídia ao fim da vida útil ou da mídia reutilizável?

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Monitorar e testar as redes regularmente</p> <p><i>Requisito 10: acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do titular do cartão.</i></p> <p><i>Requisito 11: testar regularmente os sistemas e processos de segurança.</i></p>	<ul style="list-style-type: none"> ▪ Como as atividades são rastreadas até o pessoal do cliente individual ou o pessoal do provedor individual? ▪ Os componentes específicos do sistema usados por um cliente em um determinado momento podem ser identificados? ▪ Que tipos de eventos são registrados nos registros de auditoria? ▪ Como os registros de auditoria são correlacionados entre os ambientes do cliente (como uma imagem de VM) e a infraestrutura do provedor (como o hipervisor ou o sistema subjacente)? ▪ Como os registros de auditoria são monitorados e revisados? ▪ Como os relógios são sincronizados entre instâncias virtuais e sistemas/hardware subjacentes? ▪ Como os testes de tecnologias wireless são realizados e gerenciados? ▪ Como todas as variações de imagens VM (incluindo VMs inativas) são varridas em busca de vulnerabilidades? ▪ Quais defesas estão em vigor para proteger contra ataques internos (originários da rede do provedor ou da rede de outros clientes) e ataques externos (originários da internet ou de outra rede pública)? ▪ O teste de penetração é realizado em diferentes camadas do ambiente (por exemplo, entre VMs e a rede de gerenciamento do provedor, ou entre clientes em infraestrutura compartilhada)? ▪ Como os testes de segurança são gerenciados para a infraestrutura do provedor versus ambientes do cliente? <ul style="list-style-type: none"> ○ Que testes os clientes têm permissão para realizar em seus sistemas voltados para a internet? ○ Como os clientes são impedidos de realizar testes de penetração nos ambientes de outros clientes?

Requisito do PCI DSS	Considerações para ambientes em nuvem
<p>Manter uma Política de Segurança de Informações</p> <p><i>Requisito 12: manter uma política que aborde a segurança das informações para todas as equipes.</i></p>	<ul style="list-style-type: none"> ▪ Como o provedor identifica possíveis riscos? ▪ Os clientes são notificados após alterações nas políticas de segurança e privacidade do provedor? ▪ O provedor tem mecanismos em vigor para garantir que procedimentos operacionais seguros sejam seguidos? ▪ Como o provedor faz a triagem do pessoal? <ul style="list-style-type: none"> ○ Diferentes níveis de triagem são usados para diferentes funções ou regiões? ○ A triagem abrange todos os funcionários com acesso físico aos data centers em todos os locais? ▪ O provedor terceiriza qualquer aspecto do serviço em nuvem para outros provedores (por exemplo, armazenamento de dados, serviços de segurança etc.)? ▪ Quais medidas são tomadas para garantir que as políticas de segurança do provedor sejam mantidas por seus provedores terceirizados? ▪ Quais são os processos para detectar, avaliar, encaminhar e responder a possíveis violações? <ul style="list-style-type: none"> ○ Quais são os mecanismos para que os clientes notifiquem uma suspeita de violação? ○ Quais critérios são usados para definir se um incidente ou uma violação realmente ocorreu? ○ Quais notificações são fornecidas e quando? ○ Como uma violação em um cliente afetaria outros clientes na mesma infraestrutura? ○ Como as evidências são coletadas, gerenciadas e compartilhadas? ▪ O que acontece com os dados do cliente em caso de violação dos sistemas do provedor? ▪ Os dados de um cliente podem ser coletados como parte da investigação de violação de outro cliente (ou provedor) (por autoridades ou investigadores terceirizados)? ▪ Os processos, sistemas e instalações de recuperação de desastres estão implementados com os mesmos controles de segurança que os ambientes de produção?
<p>Apêndice A1: requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada</p>	<ul style="list-style-type: none"> ▪ Como o isolamento é mantido em diferentes camadas, incluindo entre máquinas virtuais, máquinas físicas, redes, sistemas de armazenamento (por exemplo, redes de área de armazenamento), redes de gerenciamento e sistemas de suporte? ▪ Quais controles estão implementados para prevenir o vazamento de dados entre clientes, e entre o cliente e o provedor? ▪ Há mecanismos de isolamento de recursos instalados?

Apêndice E: considerações sobre segurança técnica

As considerações sobre segurança técnica para ambientes em nuvem geralmente incluem todas aquelas que se aplicam às tecnologias de virtualização, bem como aquelas diretamente relacionadas aos diferentes modelos de implantação e categorias de serviços em nuvem.

E.1 Tecnologias de segurança em evolução

Conforme mencionado acima, as considerações sobre segurança de virtualização também se aplicam a ambientes de nuvem. Há muitos recursos do setor, incluindo as "Diretrizes de virtualização do PCI DSS", disponíveis no site do PCI SSC, que discutem as considerações de segurança para o uso de tecnologias virtuais. Algumas dessas considerações são:

- É difícil manter configurações atualizadas e seguras em máquinas virtuais quando elas são ativadas e desativadas em ciclos rápidos – máquinas virtuais que estejam inativas por qualquer período podem estar indevidamente protegidas ou podem introduzir vulnerabilidades de segurança quando ativadas.
- As soluções de segurança e monitoramento para redes virtuais ainda estão evoluindo e não são tão maduras quanto aquelas disponíveis para redes físicas; por exemplo, testes contínuos de segmentação entre as redes de locatários da nuvem.

Além disso, as funções tradicionais do software de segurança e do dispositivo de segurança geralmente não se expandem bem para um ambiente de nuvem. Por exemplo:

- O gerenciamento de tráfego entre VMs que não passa por controles de segurança tradicionais baseados em rede pode exigir o uso de controles de segurança baseados em host adicionais para monitorar e controlar o tráfego.
- Soluções tradicionais de segurança de software baseadas em agente que não são projetadas para ambientes virtualizados podem causar problemas operacionais. Por exemplo, agentes de software, como aqueles usados com frequência para proteção antivírus, utilizam uma pequena porcentagem de recursos de memória e processamento; isso pode resultar em uma grande sobrecarga quando vários agentes são instalados em várias VMs no mesmo host.
- Varreduras programadas ou atualizações ocorrendo simultaneamente em várias VMs podem resultar em uma carga extrema no sistema subjacente e reduzir o desempenho geral de todas as VMs hospedadas.

E.2 Multilocação

Em um ambiente de nuvem multilocatário, os clientes geralmente não têm conhecimento dos outros clientes com quem compartilham recursos (por exemplo, infraestrutura virtual, armazenamento de dados etc.), ou como outros clientes estão protegendo (ou não protegendo) seus ambientes que acessam os recursos compartilhados.

O provedor deve realizar um teste de segmentação em um ambiente multilocatário para garantir que os locatários da nuvem sejam isolados uns dos outros (consulte a Seção 6.5.3.3, "Testes de segmentação" para mais informações).

Se clientes displicentes podem representar um risco para outros clientes usando o mesmo provedor dependerá, em grande parte, dos controles que o provedor tem em vigor para separar os clientes uns dos outros e para monitorar e detectar atividades suspeitas na infraestrutura compartilhada

e entre os ambientes do cliente. Antes de contratar um provedor, os clientes devem considerar como o provedor verifica se seus clientes são quem afirmam ser e como o provedor detecta comportamentos potencialmente suspeitos quando os clientes forem integrados. Os clientes também devem perguntar ao provedor quais controles ele tem em vigor para garantir que a postura de segurança de um cliente não possa afetar a postura de segurança de outro cliente.

E.3 Internet das Coisas e computação em névoa

Dispositivos "inteligentes", como telefones celulares, tablets, dispositivos vestíveis, sensores inteligentes e dispositivos da IoT são cada vez mais usados para aceitar e processar pagamentos. Embora esses dispositivos dependam do ecossistema baseado em nuvem, eles frequentemente usam a computação em névoa ("névoa") como uma camada entre si e o back-end da nuvem.²⁰

A computação em névoa ou a rede em névoa é uma arquitetura emergente para computação, armazenamento, controle e rede que distribui esses serviços mais próximos dos usuários finais ao longo do contínuo da nuvem para as coisas.²¹ De um ponto de vista arquitetônico, a névoa fornece recursos de computação mais próximos dos end-points que produzem dados na borda. Os dispositivos na computação em névoa (nós de névoa) tendem a estar em uma implantação amplamente distribuída, com um número muito grande de nós posicionados para ingestão e processamento dos dados próximos à fonte (ou seja, dispositivos da IoT), fornecendo interação com o back-end da nuvem.

A computação em névoa pode ser vista como uma extensão da arquitetura de computação tradicional baseada em nuvem, modelos de serviço e categorias. Como na computação em nuvem, os nós de névoa são implantados como nós privados, comunitários, públicos ou híbridos, apoiando as categorias de serviço SaaS, PaaS e IaaS. Portanto, os princípios e as orientações nesse documento são aplicáveis aos dispositivos da IoT e aos ecossistemas de computação em névoa.

E.4 Redes definidas por software

Normalmente, a estrutura e a segmentação de uma rede são definidas com o uso de dispositivos de rede, incluindo firewalls e switches. SDN é a capacidade de abstrair funções de rede de nível inferior ao expor a capacidade de alto nível através de uma API. A SDN separa a atividade da rede em um plano de controle e em um plano de dados, com o plano de dados executando diretamente funções de transporte de dados e o plano de controle atuando como um ponto central separado para chamadas API a fim de definir o gerenciamento da camada de dados. As SDNs frequentemente são usadas para a microsegmentação, que é a capacidade de definir um circuito ponto a ponto entre dois nós, impedindo-os de interagir com outros sistemas e impedindo que outros sistemas interajam com eles sem uma política explicitamente adicionada.

²⁰ Michaela Iorga, Larry Feldman, Robert Barton, Michael J. Martin, Nedim Goren, and Charif Mahmoudi, *Fog Computing Conceptual Manual, NIST Special Publication 500-325*, (Gaithersburg: National Institute of Standards and Technology, March 2018). <https://doi.org/10.6028/NIST.SP.500-325>.

²¹ Open Fog Consortium, <https://www.openfogconsortium.org>.

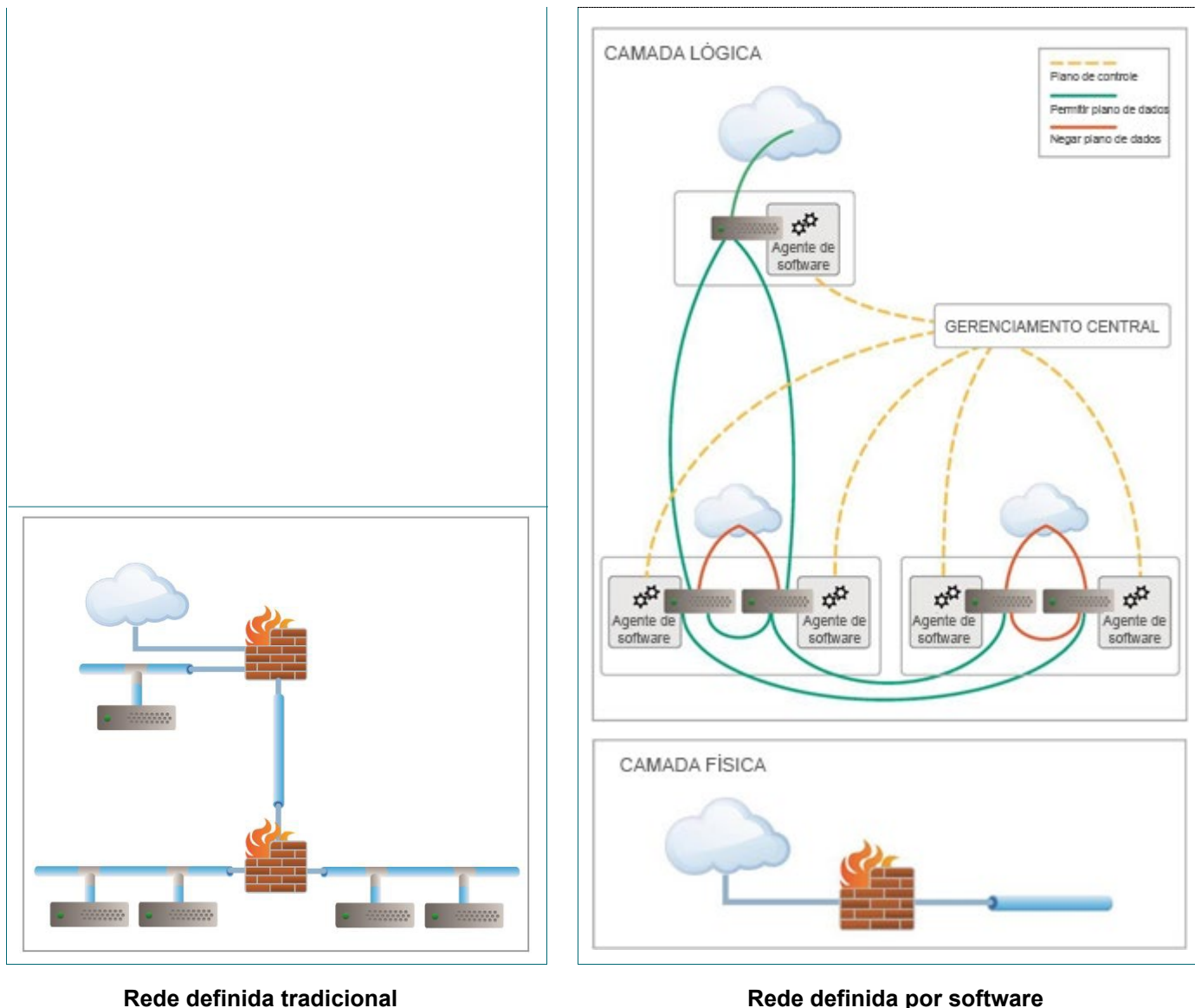


Figura E-1: Comparação de SDN e rede tradicional

Os ambientes SDN devem ser avaliados de forma consistente, sejam eles fornecidos por um provedor externo (em uma situação de nuvem pública ou híbrida) ou por um provedor interno (em uma situação de nuvem privada no local). O provedor de SDN deve manter uma separação das tarefas do consumidor SDN (seja um cliente externo ou uma unidade de negócios dentro de uma organização), mesmo que estejam na mesma organização, para garantir que o provedor SDN não seja capaz de alterar a topologia de rede ou regras fora do que está acordado com o cliente.

Em ambientes SDN multilocatários, os consumidores SDN devem ser separados logicamente uns dos outros no SDN, e cada consumidor SDN só deve ser capaz de atualizar as políticas de rede aplicáveis aos seus sistemas e não deve ter visibilidade das políticas gerenciadas por outros consumidores SDN.

Evidências típicas para demonstrar a força de uma solução devem incluir:

- O código e a sintaxe reais passados para as APIs para elaborar as políticas de tráfego
- O gerenciamento de mudanças que apoia o código, incluindo os processos para revisá-lo, aprová-lo, confirmá-lo e testá-lo
- Uma comparação do código fornecido e as políticas ativadas no plano de controle
- Testes de penetração do plano de dados para confirmar que não é possível ignorar as políticas aplicadas e os controles de microsegmentação
- Testes de penetração do plano de controle para validar que as políticas não podem ser atualizadas fora do processo de revisão estabelecido

Ao observar as melhores práticas, os limites entre uma SDN e uma rede tradicional devem ser bem demarcados para garantir consistência na forma como os controles são aplicados.

Ao usar SDN, é necessário garantir que a intenção de todos os requisitos seja atendida pelo provedor do SDN ou pelo cliente do SDN; por exemplo, funções IDS/IPS, ofuscação de endereços IP internos, fortalecimento da infraestrutura de SDN, sincronização, segurança da trilha de auditoria centralizada e revisão periódica de registros.

E.5 Sistemas de detecção de invasão (Intrusion Detection Systems, IDS)/sistemas de prevenção de invasão (Intrusion Prevention Systems, IPS)

Como o acesso do cliente aos dados de nível de rede pode ser severamente restrito em ambientes de nuvem, a responsabilidade pelo rastreamento de invasões na camada de rede geralmente será do provedor, como a única entidade que tem privilégios suficientes para fazer isso em toda a infraestrutura subjacente.

Dependendo do tipo de camada de serviço (ou seja, IaaS, PaaS ou SaaS), os provedores podem oferecer acesso ao sistema de detecção de invasão (intrusion detection system, IDS), ao sistema de prevenção de invasão (intrusion prevention system, IPS) ou aos dados das ferramentas que usam para permitir que os clientes do serviço em nuvem tenham recursos de auditoria e de emissão de alertas:

- **SaaS:** como o acesso do cliente ao tráfego de rede de baixo nível é impossível, ele deve contar com os provedores para IDS/IPS, monitoramento e emissão de alertas.
- **PaaS:** os clientes não têm acesso direto à funcionalidade IDS/IPS, pois normalmente estão fora da plataforma e, portanto, devem contar com provedores para IDS/IPS.
- **IaaS:** o cliente e os provedores têm responsabilidades compartilhadas e devem avaliar a implantação de IDS/IPS em locais-chave no ambiente IaaS, por exemplo, em máquinas virtuais ou contêineres, sistemas de hipervisor/host, rede virtual ou infraestrutura de rede subjacente.

Outras alternativas para implementar a detecção de invasão ou a prevenção de invasão nos ambientes de nuvem incluem o bloqueio de tráfego para recursos definidos específicos com base na função em vez de IP (alterações dinâmicas na nuvem tornam o bloqueio de IPs problemático: o intervalo é muito grande ou muito pequeno), usando uma solução IPS/IDS baseada em host na imagem da instância ou no contêiner, ou roteando o tráfego de rede por meio de um provedor de serviços de IPS/IDS de terceiros (ou seja, um provedor de serviços de SECaaS). Essas e outras alternativas devem ser avaliadas pelo provedor, cliente e o avaliador envolvido na validação de conformidade para garantir que atendam à intenção de todos os requisitos aplicáveis do PCI DSS.

E.6 Acesso e introspecção do hipervisor

Em ambientes de nuvem grandes pode ser difícil acompanhar quais hipervisores estão executando quais VMs, pois as VMs podem ser dinamicamente atribuídas em um conjunto de hipervisores com base nas necessidades de balanceamento de carga. A configuração e o acesso do hipervisor são especialmente importantes, pois um hipervisor fornece um único ponto de entrada para todas as VMs e pode ser usado para obter acesso a dados e recursos confidenciais em VMs separadas.

Uma consideração adicional é o grau em que o hipervisor é usado para fornecer funcionalidade de segurança às VMs. Por exemplo, um hipervisor fortalecido simples pode ser muito seguro, mas oferecer recursos de segurança limitados, enquanto um hipervisor mais complexo, com recursos de segurança e funcionalidade aprimorada, possivelmente poderia apresentar um risco maior se fosse comprometido.²²

A funcionalidade que permite que o hipervisor controle e monitore a atividade de VMs individuais externamente às VMs é chamada introspecção. A introspecção do hipervisor expande a funcionalidade do hipervisor para permitir uma análise mais aprofundada dos dados sendo processados pela VM, e normalmente inclui visibilidade dos arquivos de dados armazenados, bem como monitoramento do tráfego da rede, da execução da memória e do programa, e outros elementos da VM.

Dependendo da tecnologia específica implementada, a introspecção pode fornecer ao provedor²³ um nível de auditoria em tempo real da atividade da VM que, do contrário, seria inalcançável. Isso pode ajudar o provedor a monitorar e a detectar atividades suspeitas dentro e entre VMs. Além disso, a introspecção pode facilitar implementações eficientes em nuvem dos controles de segurança tradicionais, por exemplo, funções de segurança gerenciadas do hipervisor, como proteção contra malware, controles de acesso, firewall e detecção de invasão entre VMs.

²² Tim Mather, Don't Bloat the Hypervisor! What to know about Introspection (Webinar), 2011.

²³ Joe Security LLC, Joe Security's Blog, "Level Up: Introducing Hypervisor based Inspection in Joe Sandbox," <https://joesecurity.org/blog/68779205757215410> (20 June 2017).

Dois desafios em potencial relacionados à introspecção são a possibilidade de ela ignorar controles de acesso baseados em funções e de ser usada sem deixar uma trilha de auditoria forense dentro da própria VM. Por exemplo, para visualizar um arquivo de dados, um usuário normalmente faz a autenticação na VM, resultando em uma trilha de auditoria de autenticação e garantindo que o acesso do usuário seja controlado de acordo com as permissões definidas do usuário. Se o registro de acesso dos arquivos estiver ativado na VM e o usuário visualizar um arquivo, o acesso será gravado para mostrar o que foi acessado, por quem e quando. Com a introspecção, os arquivos podem ser acessados a partir do estado privilegiado do hipervisor. Como nenhuma autenticação na própria VM é necessária, o acesso dos arquivos não deixa nenhuma trilha de auditoria na VM e a VM não contém nenhuma evidência de que o arquivo foi acessado. Neste exemplo, o acesso precisaria ser registrado através da própria ferramenta de introspecção, o que normalmente não estaria no controle do cliente. Embora isso seja um problema secundário dentro de um ambiente de nuvem privada, é uma consideração importante para os clientes de serviços de nuvem pública. A pesquisa foi apresentada sobre a detecção de atividades do hipervisor dentro de uma VM ²⁴ e introspecção de hipervisor assistida por hardware.²⁵

Além disso, como a introspecção é projetada para ter visibilidade total em cada VM, pode ser difícil restringir esse acesso a apenas arquivos ou programas específicos na memória. Qualquer pessoal (por exemplo, funcionários do provedor ou possivelmente outros clientes hospedados) com acesso à função de introspecção potencialmente poderia ter acesso a dados e processos em qualquer VM executando naquele hipervisor.

Portanto, o acesso de introspecção deve ser cuidadosamente gerenciado, controlado e monitorado para garantir que o acesso e a separação de tarefas baseadas em função sejam mantidos. Por exemplo, a capacidade de configurar a auditoria de introspecção não deve estar disponível para o pessoal com a capacidade de acessar VMs hospedadas através da ferramenta de introspecção.

Os provedores podem utilizar produtos que forneçam Introspecção da máquina virtual (Virtual Machine Introspection, VMI, também chamada introspecção do convidado). Os provedores têm mercados com produtos de segurança, como aqueles para AV, IPS e FIM, que fornecem proteção a partir de um dispositivo de fonte central para máquinas virtuais com implementações mínimas ou sem agentes. Esses produtos geram registros que podem ser analisados por SIEMs de informações de segurança e gerenciamento de eventos, e participam de uma implementação de alertas.

²⁴ Gary Wang, Zachary J. Estrada, Cuong Pham, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Hypervisor Introspection: A Technique for Evading Passive Virtual Machine Monitoring," University of Illinois at Urbana-Champaign, <https://www.usenix.org/system/files/conference/woot15/woot15-paper-wang.pdf>

²⁵ Jiangyong Shi, Yuexiang Yang, and Chuan Tang, "Hardware assisted hypervisor introspection," 17 May 2016, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4870477/#Sec21>.

Os provedores que usam produtos baseados em introspecção devem ser capazes de fornecer aos seus clientes todos os registros de introspecção aplicáveis para o ambiente do cliente, incluindo, entre outros, detalhes de autenticação, solicitações de acesso ao disco e à memória, e chamadas API. Todas as atividades de introspecção devem ser mapeadas para a conta de usuário individual que executa a atividade, e os registros devem ser analisados continuamente para garantir que a integridade e a confidencialidade dos dados do cliente tenham sido mantidas.

Onde a introspecção é usada por um provedor terceirizado, os clientes podem querer considerar a implementação de controles de segurança em nível de dados (como criptografia forte com todas as operações de armazenamento e criptografia/descriptografia de chaves externas ao serviço em nuvem) para evitar a exposição de dados confidenciais aos recursos de monitoramento aprimorados que a introspecção fornece.

E.7 Contêineres

A containerização é uma tecnologia cada vez mais popular para executar com eficiência muitas instâncias de um servidor ou aplicativo. Possui propriedades de isolamento de recursos, segurança e proteção semelhantes às das máquinas virtuais, mas sem as despesas iniciais de memória e de desempenho inerentes a hipervisores no nível do sistema. As plataformas de orquestração de contêineres estão se tornando uma oferta de serviço cada vez mais popular que permite aos clientes iniciar uma instância ou um grupo de contêineres e controlar dinamicamente a capacidade de saída de computação.

Os contêineres são projetados para implantação como grupos de sistemas muito leves e de curta duração. Isso oferece velocidade e escalabilidade ao aumentar a quantidade de contêineres no grupo dinamicamente. Por causa disso, os controles devem focar nos modelos de imagem e no grupo como um todo, e não nos contêineres individuais dentro do grupo.

As organizações devem examinar sua tecnologia de orquestração de contêineres para confirmar que ela inclui pelo menos o seguinte:

- Controles de acesso tanto para a estrutura de orquestração quanto para os próprios contêineres de modo que cargas de trabalho diferentes não tenham acesso a chaves, tokens de identidade e outras informações confidenciais usadas por outros contêineres no cluster.
- Isolamento de processo dos contêineres em execução com base em tecnologias padrão do setor, como namespaces de kernel () e CGroups(). As melhores práticas incluem controles para aplicar verificações de permissão de kernel em processos privilegiados (às vezes chamados recursos).
- Restrição de acesso de contêineres a sistemas de arquivos host e restrição de acesso a sistemas de arquivos de contêineres por outros contêineres.

- Um firewall de chamada de sistema em pleno funcionamento e *específico do contêiner* que tem uma regra usual de *negação padrão* e permite apenas chamadas de sistemas que sejam seguras e conhecidas. Como alternativa, recursos de segurança de kernel como AppArmor, SELinux, RSEC e Modo de Computação Segura (seccomp) podem ser usados para permitir que apenas chamadas do sistema sejam consideradas seguras.
- O isolamento forte administrativo e da rede entre contêineres que hospedam cargas de trabalho diferentes com base em uma interface de rede específica do contêiner, como a interface docker0 e redes definidas por software (consulte a Seção E.4, “Redes definidas por software”).
- Quando possível, o isolamento de kernel, conforme oferecido por algumas soluções de contêiner baseadas em hipervisor, para atender às recomendações das diretrizes de virtualização do PCI DSS²⁶ para cargas de trabalho de modo misto.
- A capacidade de gerar uma auditoria de aprovações de acesso e revisão para o sistema de orquestração de contêineres, demonstrando que o acesso é limitado ao menor número de pessoas apropriadas para as cargas de trabalho dentro do escopo.
- Como a maioria das soluções de contêineres utiliza metodologias de desenvolvimento de integração contínua/implantação contínua, a integridade do pipeline de CI/CD e o controle de alterações devem ser avaliados para validar a força dos controles acima (consulte a Seção E12, “Detecção de alterações para sistemas baseados em nuvem”).
- O repositório que armazena as imagens do contêiner deve ser gerenciado com segurança e a criação das imagens processadas sob gerenciamento rigoroso das alterações.
- As imagens usadas para os contêineres devem ser corrigidas durante o processo de criação de imagem (ou seja, modelo de imagem) e devem ser submetidas à avaliação de vulnerabilidade padrão antes de incorporar a imagem no repositório.
- Quando possibilitado pelo aplicativo, contêineres somente para leitura devem ser usados.

Como os contêineres podem ser usados para alcançar um nível semelhante de execução, as organizações podem optar por usá-los para segmentar seu escopo do PCI DSS de uma maneira semelhante às máquinas virtuais. O cliente deve validar que a tecnologia de orquestração de contêineres ou a solução oferecida pelo provedor tem todos os recursos necessários para isolar completamente os contêineres. Se o isolamento de cargas de trabalho dentro de um cluster não puder ser garantido através de controles técnicos, o cliente deve considerar a implantação de cargas de trabalho em clusters separados e específicos da carga de trabalho. Alguns provedores podem oferecer a capacidade para um cliente individual orquestrar vários clusters, mas alguns provedores podem não oferecer isso e todas as cargas de trabalho são implantadas em clusters compartilhados de carga de trabalho mista. Nesse último caso, um cliente pode precisar considerar contas de clientes específicas da carga de trabalho para fornecer o isolamento necessário.

²⁶ Grupo de interesse especial de virtualização e PCI Security Standards Council, Diretrizes de virtualização do PCI DSS (PCI SSC, junho de 2011), https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf.

Validar que uma solução de contêiner tem a força de isolamento necessária em vigor significa escolher uma solução de código aberto e comercial aprovada e confiável que tenha demonstrado um forte histórico de segurança ao longo do tempo, em vez de desenvolver uma tecnologia de contêiner internamente.

Muitas organizações têm enfrentado dificuldades para atender aos requisitos trimestrais e anuais do PCI DSS em relação a contêineres que podem ser criados, executados, descontinuados e destruídos em questão de dias ou horas. Em alguns casos, uma verificação da frota de contêineres pode ocorrer toda semana, como para o monitoramento da integridade de arquivos, seguindo o Requisito 11.5 do PCI DSS, ou no decorrer de semanas ou meses no caso de um teste de penetração. Nos casos em que o ciclo de vida do contêiner for menor do que a duração de um determinado controle do PCI DSS, considere obter uma amostragem das instâncias em execução em todas as imagens do contêiner dentro do escopo (consulte a Seção E.9, “Inventário e controle de recursos elásticos” para mais informações).

Além disso, como parte do pipeline de instanciação do contêiner, uma organização pode querer realizar um teste de vulnerabilidade (consulte a Seção, 6.5, “Gestão de vulnerabilidades”) para abordar o desafio de implementar controles de segurança em um ambiente altamente fluido e elástico, bem como para avaliar o impacto sobre os requisitos do PCI DSS de acordo com o Requisito 6.4.5 do PCI DSS.

E.8 Infraestrutura de desktop virtual na nuvem

A Infraestrutura de desktop virtual (Virtual Desktop Infrastructure, VDI) é uma tecnologia de virtualização que tem suas próprias complexidades de conformidade que são discutidas no suplemento de informações *Diretrizes de virtualização do PCI DSS*. Quando fornecido por um provedor como uma oferta de serviços na nuvem, essas complexidades são compostas. O uso dessa tecnologia é discutido neste contexto estritamente no que diz respeito à entrega de serviços de VDI por um provedor, doravante referido como um Desktop como serviço (Desktop-as-a-Service, DaaS).

Diferentes configurações de host podem ser fornecidas por um provedor, o que pode afetar de forma única a determinação do escopo do ambiente ou as responsabilidades do provedor de serviços referentes aos muitos componentes envolvidos, incluindo a estação de trabalho, sistema host, sistema operacional convidado, rede virtual, hipervisor, armazenamento de imagem e armazenamento de arquivos:

- **Desktop remoto tradicional:** embora não sejam comumente considerados VDI, desktops remotos tradicionais, serviços de terminal ou jump servers também podem ser fornecidos usando virtualização ou como serviço por parte de um provedor. Este modelo é abordado no Suplemento de informações do PCI sobre determinação de escopo e segmentação²⁷ para estações de trabalho de administrador.

- **VDI tradicional:** o servidor de desktop virtual está instalado em um sistema operacional convidado. Todos os usuários compartilham um único espaço de host e memória, embora imagens e arquivos possam ser armazenados e acessados a partir de outros locais de rede, como Armazenamento conectado à rede (Network Attached Storage, NAS), Redes de área de armazenamento (Storage Area Networks, SAN) ou Rede de área de armazenamento virtual (Virtual Storage Area Network, VSAN).
- **Espaço de trabalho VDI em nível de aplicativo:** os espaços de trabalho VDI sem estado não dependem mais de um único sistema operacional convidado. Em vez disso, os componentes da área de trabalho virtual podem ser hospedados diretamente pelo hipervisor, tornando possível para os aplicativos individuais que compreendem a "experiência de desktop" a serem hospedados e servidos a partir de hipervisores, hosts e repositórios de armazenamento separados que residem em segmentos de rede virtuais ou zonas de segurança distintas. Os provedores que fornecem VDI sem estado devem consultar a orientação existente sobre implicações da entrega de serviço de modo misto para confirmar o escopo de cada aplicativo e armazenamento de dados, e atender a todos os requisitos de isolamento e requisitos de testes de segmentação necessários para limitar o escopo (se aplicável).

Recursos DaaS, como imagens de disco e hipervisores, podem existir em redes separadas. Para garantir a enumeração de todos os sistemas dentro do escopo, todas as provisões de rede para sistemas CDE devem seguir caminhos designados que são identificados pelos fluxogramas de rede e de dados da parte responsável.

Quando os sistemas host e hipervisores são mantidos e provisionados por um provedor, a responsabilidade pela configuração, pela correção, pelo monitoramento e pelos testes seguros geralmente recai sobre o provedor e deve ser identificada no AOC do provedor ou na matriz de responsabilidades, ou em ambos. Da mesma forma, onde as imagens são mantidas pelo provedor, o armazenamento e o acesso à rede a imagens devem ser confirmados pelo AOC do provedor (consulte as Seções 5.2, "Verificação do escopo dos serviços e componentes validados do PCI DSS" e 5.3, "Verificação dos controles do PCI DSS gerenciados pelo provedor de serviços em nuvem" para mais informações).

Recomenda-se que as imagens de disco do VDI para CDE e não CDE não sejam combinadas para garantir que os componentes do sistema não CDE não possam montar volumes de CDE – sistemas que residem ou acessam imagens de disco de CDE e não CDE devem ser considerados dentro do escopo para o PCI DSS. Para reduzir o escopo da avaliação do PCI DSS, o provedor deve ter a segmentação necessária em vigor e assumir a responsabilidade expressa por esses controles. Para provedores que fornecem hospedagem compartilhada de serviços de VDI, a solução de hospedagem deve impor a separação apropriada dos locatários da nuvem para ambientes de nuvem multilocatário (consulte a Seção E2, "Multilocatário" para mais informações).

Como as configurações do servidor variam, as configurações de estação de trabalho do cliente podem ter uma gama significativa de controles aplicáveis. Os três tipos de estações de trabalho de VDI mais comuns incluem:

²⁷ PCI Security Standards Council, Orientação para determinação do escopo e segmentação de rede do PCI DSS (PCI SSC, dezembro de 2016), https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

- **Zero Client:** esses sistemas fornecem pouco mais do que vídeo, teclado e interface de mouse para o host de rede. Sem um processador ou espaço de memória para hospedar malware, as configurações de zero client oferecem uma superfície de ataque mínima e a interceptação de dados confidenciais exigiria a invasão física no ambiente. Assim que os controles físicos e os recursos do terminal forem confirmados, um avaliador pode considerar que nenhum controle adicional é necessário.
- **Thin Client:** um sistema operacional leve geralmente é instalado nesses sistemas para suportar a conexão ao host, mas também pode incluir suporte para aplicativos configuráveis que são executados localmente. Por esse motivo, estações de trabalho thin client podem ser consideradas dentro do escopo e sujeitas a muitos controles de estação de trabalho. Certos requisitos do PCI DSS, como o Requisito 5, podem ser considerados não aplicáveis se o sistema operacional subjacente não for comumente afetado por malware. No entanto, não é suficiente presumir que as estações de trabalho thin client estão inteiramente fora do escopo para esses controles.
- **Estação de trabalho convencional:** uma estação de trabalho completa que suporta conexões de desktop remoto ao CDE é considerada totalmente dentro do escopo como uma estação de trabalho de administrador. O PCI Security Standards Council publicou o Suplemento de informações *Orientação para determinação do escopo e segmentação de rede do PCI DSS*, cujo objetivo é proporcionar mais compreensão dos princípios de determinação do escopo e de segmentação para estações de trabalho de administrador, conforme aplicável ao ambiente do PCI DSS.²⁸

Em cada uma das situações acima, é fundamental que o provedor e o cliente tenham responsabilidades claramente comunicadas e diagramas de rede detalhando limites de segmentação e locais de rede pertencentes ao hardware físico, hipervisor, redes virtuais, sistema operacional convidado, VDI/serviço de desktop remoto, imagens de disco e todos os binários e configurações de aplicativos. Além disso, como as ofertas DaaS multilocatário são desenvolvidas em ambientes de modo misto e entregues como um serviço usando níveis variados de capacidade de acesso do cliente, a documentação completa e a comunicação clara das responsabilidades se tornam essenciais para garantir que todas as proteções relevantes sejam confirmadas como estando em vigor e mantidas pelas partes responsáveis.

²⁸ PCI Security Standards Council, *Orientação para determinação do escopo e segmentação de rede do PCI DSS* (PCI SSC, dezembro de 2016), https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

E.9 Inventário e controle de recursos elásticos

Arquiteturas de nuvem projetadas para se expandir elasticamente podem apresentar desafios que afetam vários requisitos do PCI DSS, incluindo os Requisitos 2.4, 6.4, 10.2.7, 11.3.1 e 11.3.2, entre outros. Para melhor avaliar a adesão de ambientes gerados elasticamente aos requisitos do Padrão de Segurança de Dados do PCI, uma organização deve avaliar os controles em relação à automação de escalabilidade.

- As imagens modelo a partir das quais os recursos elásticos são instanciados devem ser revisadas quanto à adesão aos padrões de configuração do sistema e aos controles de segurança (por exemplo, Requisitos 2.1, 2.2 e 5.1 do PCI DSS).
- O ambiente ao qual os recursos elásticos são implantados deve ser avaliado quanto à adesão às regras de segmentação de rede (por exemplo, Requisitos 1.2, 1.3 e 7.2 do PCI DSS).
- Como o inventário dos componentes do sistema (conforme exigido pelo Requisito 2.4 do PCI DSS) pode mudar dinamicamente, a automação elástica deve registrar todas as atividades de criação e de destruição do sistema para fornecer a capacidade de emitir notificação sobre o inventário ao longo do tempo ou em uma instância específica.
- O sistema deve ser capaz de fornecer um relatório de instantâneo do inventário atualmente implementado (Requisito 2.4 do PCI DSS) para comparar com os arquivos de registro como demonstração da integridade da auditoria do inventário.
- Como alternativa à revisão da gestão de alterações (Requisito 6.4 do PCI DSS) em relação a eventos elásticos individuais, uma organização poderia revisar a gestão de alterações em relação às regras que regem eventos elásticos e a gestão de alterações em relação aos sistemas de automação, incluindo as imagens modelo e os sistemas de provisionamento.
- A administração da automação elástica, incluindo o desenvolvimento do pipeline de automação elástica, deve ser revisada quanto ao forte controle de autenticação e à auditoria das atividades (Requisitos 8.1, 8.2 e 8.3 do PCI DSS).
- Considere incluir uma varredura de vulnerabilidade no início de uma instância, API de contêiner ou lançamento de serviço para fornecer um registro do artefato e uma revisão do impacto da alteração.
- Os testes de penetração (Requisito 11.3 do PCI DSS) devem incluir a automação de provisionamento e orquestração, bem como o ambiente provisionado, incluindo controles em relação aos modelos de imagem e à criação de redes dinâmicas.

E.10 Criptografia de dados e gerenciamento de chaves criptográficas

Em um ambiente de nuvem pública, os dados de um cliente normalmente são armazenados com dados pertencentes a vários outros clientes. Isso torna uma nuvem pública um alvo atraente para invasores, já que o ganho em potencial pode ser maior do que o obtido com o ataque a várias organizações individualmente. A criptografia de nível de dados forte deve ser aplicada a todos os dados confidenciais ou potencialmente confidenciais armazenados em uma nuvem pública. Como o comprometimento de um provedor pode resultar em acesso não autorizado a vários armazenamentos de dados, recomenda-se que as chaves criptográficas usadas para criptografar/descriptografar dados confidenciais sejam armazenadas e gerenciadas independentemente do serviço em nuvem onde os dados estão localizados. No mínimo, os servidores de gerenciamento de chaves devem estar localizados em um segmento de rede separado e protegidos com credenciais de acesso separadas das VMs que estão usando as chaves e os dados criptografados com elas.

Apenas responsáveis pelas chaves definidos e autorizados devem ter acesso a chaves criptográficas. Como o acesso a ambas as chaves e aos dados criptografados fornece a capacidade de descriptografar os dados, os clientes precisarão verificar quem tem acesso a chaves criptográficas, quem tem acesso aos dados criptografados e quem tem acesso a ambos. Se um cliente compartilhar chaves de criptografia com o provedor ou incluir o provedor como um responsável pelas chaves, os detalhes das permissões e dos processos do provedor também precisarão ser revisados e verificados.

Esta consideração é particularmente crítica se as chaves criptográficas forem armazenadas ou hospedadas por um provedor terceirizado que também hospeda os dados criptografados. Se o pessoal do provedor tiver acesso às chaves do cliente e aos dados criptografados do cliente, o cliente pode ter concedido inadvertidamente a capacidade do provedor de descriptografar seus dados confidenciais.

Quaisquer dados descriptografados na nuvem podem ser inadvertidamente capturados em “clear-text” na memória de processo ou em VMs por meio de funções de manutenção em nuvem (como snapshots, backups, ferramentas de monitoramento etc.). Para evitar esse risco, os clientes podem optar por manter todas as operações de criptografia/descriptografia e gerenciamento de chaves em suas próprias instalações, e usar uma nuvem pública apenas para armazenamento dos dados criptografados.

Controles aplicáveis devem ser aplicados aos processos de criptografia, descriptografia e gerenciamento de chaves para garantir que os dados só possam ser recuperados (descriptografados) por quem está autorizado em decorrência de uma necessidade comercial definida.

Os provedores que prestam serviços de gerenciamento de chaves criptográficas para seus clientes, como o Cloud HSM (consulte a Seção E.11, “Dispositivos de criptografia segura na nuvem”) devem garantir que chaves secretas ou privadas não sejam compartilhadas entre os clientes; cada cliente deve receber uma chave exclusiva ou um conjunto de chaves. Canais seguros para acesso ao ambiente em nuvem também exigem gerenciamento de chaves adequado. Se o provedor usar imagens ou clonagem para proteger VMs, recomenda-se enfaticamente que as chaves não sejam clonadas como parte da imagem da VM – cada instância de clone ou VM deve ter sua(s) própria(s) chave(s).²⁹

Por fim, o campo de criptografia está evoluindo continuamente e novas técnicas e tecnologias criptográficas (por exemplo, divisão de bits e criptografia homomórfica) estão surgindo para proteger as informações confidenciais. Como essas tecnologias são novas, a devida diligência apropriada precisa ser realizada para pesar os prós e contras antes da decisão de adquirir ou desenvolver uma solução utilizando essas tecnologias.

E.11 Dispositivos de criptografia segura na nuvem

A necessidade de serviços criptográficos especializados para executar gerenciamento de chaves, geração de números aleatórios, criptografia ou descriptografia é aplicável a sistemas de nuvem, microserviços e outras cargas de trabalho especializadas que devem proteger os dados da conta na nuvem ou executar outros serviços de segurança. Para atender a essa necessidade, os provedores podem fornecer funções criptográficas acessíveis via API. Alguns desses serviços podem usar dispositivos de criptografia segura (secure cryptography devices, SCDs) aprovados por PTS ou FIPS do PCI, como módulos de segurança de hardware (hardware security modules, HSM). Outros podem usar serviços especializados baseados em software ou hardware não certificado para executar esses serviços. Devido à natureza dos serviços em nuvem, pode não ser prontamente aparente se a função de criptografia é realizada por um SCD real, se as certificações necessárias estão em vigor ou se determinados controles físicos e lógicos são usados pelo provedor para proteger o hardware físico.

As funções e responsabilidades por todas as funções de gerenciamento de chaves ao usar um SCD em nuvem devem ser documentadas para garantir a cobertura de todos os requisitos, incluindo a geração de chaves de força adequada, a distribuição segura de chaves do SCD e as políticas operacionais. É responsabilidade do cliente confirmar que todos os requisitos de hardware aplicáveis estão sendo atendidos pelo provedor desempenhando funções criptográficas em seu nome. Por exemplo, o PCI DSS especifica um SCD como uma forma em que uma chave usada para descriptografia dos dados armazenados da conta em repouso deve ser armazenada (Requisito 3.5.3 do PCI DSS). Um cliente pode atender a esse requisito usando o serviço de criptografia de um provedor somente se o provedor estiver usando hardware SCD real para entregar o serviço.

Da mesma forma, o provedor também é responsável por controles de segurança física, armazenamento de chaves e procedimentos de distribuição, além de políticas de criptografia documentadas. Os controles sendo atendidos pelo provedor na entrega do(s) serviço(s) em conformidade devem ser claramente identificados no AOC e na matriz de responsabilidades do provedor.

²⁹ A necessidade de chaves de host exclusivas tem sido bem documentada em vários documentos técnicos do provedor.

Quando o cliente usar chaves geradas pelo SCD, ele é responsável por documentar o uso da chave, a custódia, os controles de acesso e os mecanismos de proteção após a recuperação das chaves.

Além do PCI DSS, há outros programas do PCI SSC que têm requisitos rigorosos quanto ao uso de SCDs que atendem a certificações específicas do setor; por exemplo, PCI PTS HSM v2 e FIPS 140-2 nível 3. Exemplos de padrões atuais que incluem estipulações de hardware SCD incluem PCI P2PE, PCI PIN, PCI TSP, PCI SPoC e PCI 3DS Core Security Standard. Além disso, os requisitos para esses programas podem impor requisitos de segurança física e lógica adicionais relacionados à proteção de dispositivos aprovados. As entidades sujeitas a essas exigências devem confirmar que o provedor foi avaliado em relação a todos os requisitos de segurança física relevantes necessários para obter a conformidade com os padrões aplicáveis. Da mesma forma, os provedores podem desejar compreender e implementar proativamente os controles de segurança relevantes para esses programas do PCI se quiserem atender mercados que têm requisitos de conformidade sob seus programas (por exemplo, adquirentes, gateways).

E.12 Detecção de alterações para sistemas baseados em nuvem

Para atender ao objetivo de detecção oportuna de alterações não autorizadas no sistema e em arquivos de configuração para instâncias na nuvem, é importante incluir o monitoramento de alterações no código de provisionamento (ou seja, scripts ou modelos) usadas para a implantação de instâncias na produção, bem como implementar controles em relação a imagens usadas para a implantação de novas instâncias. Os controles em relação às imagens precisam incluir a permissão de apenas imagens fortalecidas autorizadas que foram desenvolvidas de acordo com as melhores práticas do setor (por exemplo, NIST-800-190³⁰ ou The Docker Security Benchmark³¹) e padrões de configuração da empresa a serem usados para a implantação de novas instâncias. Versões anteriores de imagens aprovadas, bem como imagens genéricas que não foram configuradas e aprovadas com segurança pelo pessoal autorizado, não devem estar disponíveis para uso para a implantação de sistemas de produção.

Nos casos em que uma instância é baseada em um sistema operacional somente leitura, como o CoreOS, o uso de ferramentas tradicionais de monitoramento da integridade de arquivos para monitorar arquivos do sistema dentro da instância de execução pode não ser mais aplicável. No entanto, tais ferramentas de detecção de alterações ainda podem ser necessárias para monitorar a integridade dos arquivos do sistema para executar instâncias que são baseadas em sistemas operacionais nos quais os arquivos de sistema e de configuração podem ser modificados.

³⁰ Murugiah Souppaya, John Morello, and Karen Scarfone, Application Container Security Guide, NIST Special Publication 800-190 (Gaithersburg, MD: National Institute of Standards and Technology, September 2017). <http://csrc.nist.gov/publications/drafts/800-190/sp800-190-draft.pdf>.

³¹ Docker, Inc., Docker Bench for Security, v1.3.3, (Docker, Inc., 2015), <https://github.com/docker/docker-bench-security>.

E.13 Segurança de interfaces de software e APIs

Interfaces de programação de aplicativos (Application programming interfaces, APIs) e outras interfaces e protocolos de software (por exemplo, SOAP e RESTful) são um componente integral da computação em nuvem, suportando interoperabilidade e entrega rápida de serviços em nuvem. As APIs podem ser configuradas para fornecer acesso a uma variedade de funções, permitindo que clientes e provedores interajam e gerenciem suas interações dentro do serviço em nuvem. Como os serviços da Web e as APIs são, por natureza, acessíveis publicamente, sua segurança é essencial para a segurança dos recursos aos quais eles fornecem acesso. Se não forem desenvolvidas, gerenciadas e protegidas adequadamente, essas interfaces podem ser exploradas ou comprometidas, resultando em comportamento inesperado e acesso potencialmente não autorizado. Por exemplo, uma API mal codificada pode resultar em protocolos de autenticação fracos, controles de acesso insatisfatórios ou capacidade de auditoria limitada. Esses pontos fracos podem levar à exposição da funcionalidade de serviço ou de dados confidenciais. Se as APIs não estiverem adequadamente seguras, elas também podem ser exploradas ou alteradas por um invasor para redirecionar fluxos de dados ou alterar o comportamento do aplicativo.

APIs e outras interfaces públicas devem ser projetadas para prevenir o uso indevido acidental e tentativas maliciosas de burlar os controles de segurança. Autenticação resiliente e controles de acesso, criptografia forte e monitoramento em tempo real são exemplos de controles que devem estar implementados para proteger essas interfaces.

Ao consumir APIs expostas por um provedor, é importante garantir que todos os requisitos aplicáveis do PCI DSS sejam atendidos. Por exemplo, todas as chamadas de API que afetam os dados do titular do cartão e o ambiente de dados do titular do cartão devem ser registradas e revisadas de acordo com o Requisito 10 do PCI DSS. Ou, ao invocar uma chamada de serviços da Web que transmita dados do titular do cartão, ela deve estar em um túnel criptografado (por exemplo, criptografia nativa SOAP ou um túnel TLS).

E.14 Gerenciamento de identidade e acesso

A identificação e a autenticação de usuários individuais para o pessoal do provedor e do cliente são essenciais para o controle de acesso e a prestação de contas (consulte os Requisitos 7 e 8 do PCI DSS). Credenciais compartilhadas (como contas de usuário e senhas) não devem ser usadas no ambiente do provedor – por exemplo, para administração e manutenção do sistema – nem contas genéricas ou compartilhadas devem ser atribuídas ou usadas pelos clientes. O uso de uma única credencial de cliente que abrange vários serviços de nuvem para esse cliente também é uma preocupação em potencial. Por exemplo, digamos que um provedor emite para um cliente uma conta de usuário e senha que tenha privilégios de administrador em um ambiente e privilégios de nível de usuário para um serviço em nuvem separado não relacionado.

O comprometimento da conta de nível de usuário do cliente no segundo ambiente poderia, portanto, conceder ao invasor acesso de nível de administrador ao primeiro ambiente. Contas e senhas de clientes devem ser exclusivas para cada serviço, e qualquer conta com privilégio elevado (como administrador) deve ser restrita para um serviço ou função específica e não usada para atividades ou acesso que não exijam tal privilégio. Em certas situações, uma autenticação multifatorial pode ser necessária para acessar recursos hospedados na nuvem. Por exemplo, o Requisito 8.2.2 do PCI DSS exige autenticação multifatorial para todo o acesso remoto à rede ao CDE, e quando os serviços de nuvem pública fazem parte do CDE de um cliente, todo esse acesso será considerado acesso remoto e exigirá autenticação multifatorial.

O PCI Security Standards Council publicou o Suplemento de informações *Autenticação multifatorial*, que fornece mais orientação sobre o tópico da autenticação multifatorial.³²

E.15 Registros e trilhas de auditoria

A capacidade de manter uma trilha de auditoria precisa e completa pode exigir registros de todos os níveis da infraestrutura, exigindo envolvimento do provedor e do cliente.

Por exemplo, o provedor pode gerenciar registros do sistema operacional no nível do sistema e registros do hipervisor, enquanto o cliente configura o registro para suas próprias VMs e aplicativos. Nessa situação, a capacidade de organizar vários arquivos de registro em eventos significativos exigiria correlação dos registros controlados pelo cliente com aqueles controlados pelo provedor.

Os provedores são responsáveis por fornecer dados de registro para recursos gerenciados pelo provedor (por exemplo, registros para componentes de infraestrutura (IaaS), registros para componentes de plataforma (PaaS), registros para componentes de software (SaaS) etc.). Os provedores devem ser capazes de separar os dados de registro aplicáveis a cada cliente e fornecê-los para cada cliente respectivo para análise sem expor dados de registro de outros clientes. Além disso, o provedor deve implementar controles para proteger os dados de registro coletados, incluindo proteção contra visualização, cópia, impressão, encaminhamento, edição e exclusão não autorizados.

Os clientes são responsáveis por garantir que o registro seja ativado para componentes que não sejam gerenciados pelo provedor (por exemplo, registros de aplicativos, registros de eventos etc.). Além disso, os clientes devem garantir que a agregação, a correlação e o monitoramento de registros estejam em vigor, conforme exigido para todas as fontes de registro, incluindo a determinação da correlação de logs e critérios de monitoramento. Em uma situação hipotética de responsabilidade compartilhada de registros, o provedor poderia gerenciar registros do sistema operacional no nível do sistema e registros do hipervisor, enquanto o cliente configura o registro para suas próprias VMs e aplicativos.

³² PCI Security Standards Council, Autenticação multifatorial (PCI SSC, fevereiro de 2017), <https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>.

A capacidade de organizar vários arquivos de registro em eventos significativos exigiria correlação dos registros controlados pelo cliente com aqueles controlados pelo provedor. Os clientes podem optar por implementar ferramentas de correlação e de monitoramento de terceiros ou implementar uma solução interna. No mínimo, a trilha de auditoria agregada deve conter informações para reconstruir os eventos listados no Requisito 10.2 do PCI DSS com detalhes suficientes para os eventos auditáveis, conforme exigido no Requisito 10.3 do PCI DSS.

Por fim, os registros coletados devem ser retidos por pelo menos um ano, de acordo com o Requisito 10.7 do PCI DSS.

O PCI Security Standards Council publicou o Suplemento de informações *Monitoramento diário eficaz de registros*, com o objetivo de fornecer mais informações e orientações para ajudar as organizações a enfrentar os desafios de manter processos eficazes de gerenciamento de registros, conforme aplicável ao ambiente do PCI DSS.³³

³³ Monitoramento diário eficaz de registros Grupo de interesse especial e PCI Data Security Standards Council, *Monitoramento diário eficaz de registros*, (PCI SSC, maio de 2016), <https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf>.

Agradecimentos

O PCI SSC gostaria de agradecer a contribuição do Grupo de interesse especial (Special Interest Group, SIG) em nuvem na elaboração deste documento, que é uma revisão do documento elaborado pelo SIG em nuvem de 2013. O SIG em nuvem de 2017 consiste em representantes das seguintes organizações:

12Feet Inc.	Carlson Wagonlit Travel
24 Solutions AB	Cautela Labs, Inc.CBIZ Security & Advisory Services, LLC
3Delta Systems, Inc.	CenturyLink
A1PlusSoft, Inc.	Chase Paymentech
AccorHotels	Cimpress
Acumera, Inc.	Cisco
Adobe	Citigroup Inc.
Advam Pty Ltd	Coalfire
Agio, LLC	Comsec
Air Liquide USA LLC	Conferma Limited
Allstate Insurance	Convergent Network Solutions, Ltd
Ascension	CSC Government Solutions/CSRA LLC
AT&T Consulting services	Datatrans AG
Ather Technology Limited, dba Cianaa Technology	Delap LLP
Automobile Club of Southern California	Delaware North Companies, Inc.
Bank of America N.A.	Direct Line Insurance Group PLC
Bank of Montreal	Dixon Hughes Goodman, LLP
Barclaycard	Dixons Carphone PLC
Basefarm A/S	Elavon Merchant Services
BBPOS	Electronic Transactions Association
BCD Travel	Emirates/Dnata
BDO USA, LLP	Equifax
Beijing UGTech Co. Ltd.	Espion LTD
Bl4ckswan S.r.l.	Experis Finance US LLC
Bravecraft (Pty) Ltd	Fiserv Solutions Inc.
BT PLC.	FiveSec Labs Limited, dba Five Security
California State University, Fullerton	Focal Point Data Risk, LLC
Capita PLC	Foregenix
Capital One Financial Corporation	Foresight IT Consulting Pty Ltd.
Card Security LLC	Games Workshop Ltd
CardConnect	Global Payments Direct Inc.

Gotham Technology Group, LLC	Optiv Security
Grant Thornton	Optomany, LTD.
Habib Bank Limited	Oracle Corporation
Harbour IT Pty Ltd	Orvis Company Inc, The
Heartland Payment Systems	Paladion Networks Private LTD
Herman Miller Inc.Hewlett Packard Enterprise Company	PAN-Nordic Card Association
HostedPCI	Parkingsoft
IBM Corporation	Payment Software Comapny (PSC)
International Certificate Authority of Management System	PayPal Inc
IQ Information Quality	PCI-PAL Limited Philips Electronics North America Corporation
Irdeto B.V.	Price and Associates CPAs, LLC, dba A-LIGN
K3DES	PricewaterhouseCoopers LLP (PWC)
Kirkpatrick Price, Inc. dba Raven Eye	Pricewaterhousecoopers Private Limited - India
KnowIT Secure AB	Protiviti
KYTE Consultants, Ltd.	Reliant Info Security Inc.
L.L. Bean, Inc.	Rock Pte. Ltd.
Little Caesars Enterprises, Inc	Rockwell Collins
Lloyds Banking Group	RSM US LLP
Macy's, Inc.	SavvyPCI
Market America Inc	Schellman & Company, LLC
McGladrey LLP	Sec-1 Ltd.
Merchant Preservation Services, LLC d/b/a CampusGuard	Secure Technology Group
National Bank of Abu Dhabi	SecureState LLC
NC Department of Natural and Cultural Resources	Securisea
NCC Group PLC	Security Metrics
NCC Services	ServerChoice
NCI Secured Intelligence	SERVIED
Netsurion	Shaw Cable Systems
Nettitude	Sikich LLP
Nintendo of America	SISA Information Security
NTT DATA INTELLILINK Corporation	SIX Payment Services Ltd
NTT Security Ltd.	Skoda Minotti Risk Advisory Services, LLC
Online Business Systems	SLM Corporation
	Sovereign Secure Ltd.
	Sprint Nextel
	Square

Stripe, Inc.	University of Colorado
Sword & Shield Enterprise Security, Inc.	University of North Carolina at Chapel Hill, The
Sysxnet Limited DBA Sysnet Global Solutions	Urbane Security
Target Corporation	Verizon
Telstra	VISTA InfoSec Private Limited
Tevora	VMware, Inc.
Thales e-Security	Vodat International Limited
The Herjavec Group Inc.	VTEX Cloud e-Commerce Platform
The Liquor Control Board of Ontario	Wells Fargo
The Regents of the University of California	WestNet Consulting Services, Inc.
Trustwave	Worldline
TSYS	WorldPay
Uber Technologies, Inc.Ubitrak	XAC Automation Corporation
UBS Card Center AG	Yusufali & Associates LLC
UL Transaction Security	ZeroFOX

Referências adicionais

Este documento se baseia nas referências adicionais a seguir. Essas fontes são recomendadas como orientação adicional sobre como proteger ambientes de computação em nuvem.

Fonte ³⁴	URL
PCI Security Standards Council (PCI SSC)	https://www.pcisecuritystandards.org
Cloud Security Alliance (CSA)	https://cloudsecurityalliance.org/
European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/
National Institute of Standards and Technology (NIST)	http://csrc.nist.gov/publications/
Information Commissioners Office (ICO)	http://www.ico.gov.uk/
ISACA	http://www.isaca.org/
ISC2 International Information Systems Security Certification Consortium, Inc.,	https://www.isc2.org/
The Open Web Application Security Project (OWASP)	https://www.owasp.org
Cloud Computing Security Research Library	http://searchcloudsecurity.com

³⁴ Links para sites de terceiros estão sujeitos à alteração.

Sobre o PCI Security Standards Council

O PCI Security Standards Council é um fórum global aberto responsável pelo desenvolvimento, gerenciamento, educação e conscientização sobre os Padrões de Segurança do PCI (PCI DSS) e outros padrões que aumentam a segurança de dados de pagamento. Criado em 2006 pelas principais bandeiras 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 provedores em todo o mundo. Para saber mais sobre como participar da proteção de dados de cartões de pagamento globalmente, acesse pcisecuritystandards.org.