



Security
Standards Council®

Padrão: Padrão de segurança de dados PCI (DSS PCI)

Data: Maio de 2017

Autor: Conselho dos Padrões de Segurança PCI (SSC PCI)

Informações complementares:
**Orientação para escopo e
segmentação de rede do
DSS PCI**

Alterações no documento

Data	Versão do documento	Descrição	Páginas
Dezembro de 2016	1.0	Versão inicial	Todos
Maio de 2017	1.1	Correção de pequenos erros tipográficos, pequenos esclarecimentos em relação à redação (com adição de nota de rodapé) na Seção 3 e correção de erros nos diagramas de Fluxo de Dados Lógicos Cenário 1 e Cenário 2 (na legenda, e diagrama e legenda, respectivamente).	5, 10, 11, 17, 22

Índice

Alterações no documento	i
1 Introdução	3
1.1 Uso pretendido e público-alvo.....	3
1.2 Terminologia.....	4
2 Compreensão do escopo e da segmentação do DSS PCI	1
2.1 Prestadores de serviços e outros terceiros.....	7
2.2 Responsabilidade pela confirmação do escopo	7
3 Definição de escopo e categorias.....	9
3.1 Verificação da segmentação de sistemas fora do escopo	13
4 Exemplo de implementações de segmentação: Serviços compartilhados.....	14
4.1 Exemplo 1: Serviços compartilhados “conectados”	15
4.2 Exemplo 2: Estação de trabalho de administração do CDE fora do CDE	18
5 Conclusão.....	24
Sobre o Conselho dos Padrões de Segurança PCI.....	25

1 Introdução

Muitas organizações lutam para entender onde são necessários controles do DSS PCI e quais sistemas precisam ser protegidos. Este documento fornece orientação para ajudar as organizações a identificar os sistemas que, no mínimo, precisam ser incluídos no escopo para o DSS PCI. Além disso, o documento fornece orientação sobre como a segmentação pode ser usada para ajudar a reduzir o número de sistemas que exigem controles do DSS PCI.

Quando se trata da definição de escopo para o DSS PCI, a abordagem da prática recomendada é começar com a suposição de que tudo está no escopo até ser verificado de outra forma. Quando implementada adequadamente, a segmentação de rede é *um método* que pode ajudar a reduzir o número de componentes do sistema no escopo para o DSS PCI. Outros métodos também podem ser eficazes na redução do número de sistemas aos quais os controles DSS PCI se aplicam e/ou o tamanho do CDE (como terceirização para um prestador de serviços terceirizado ou usando uma solução P2PE listada pela PCI). *No entanto, esses métodos não são objeto deste artigo.*

Exemplos ilustrativos de algumas abordagens de segmentação comuns estão incluídos na Seção 4. Esses exemplos destacam os impactos e as considerações do escopo do DSS PCI em torno de serviços compartilhados (como serviços de diretório) e fornecem orientação para escopo e proteção consistentes do CHD. Os exemplos neste documento não representam a única maneira de a segmentação ser usada para afetar o escopo do DSS PCI e, na verdade, pode não ser eficaz para uma determinada configuração de sistema ou rede.

Só porque um sistema não está no escopo para o DSS PCI não significa que a entidade deve deixar esse sistema desprotegido, pois ainda poderia representar um risco para a rede e os negócios da entidade. Um padrão comum observado em violações de dados é quando o invasor visa os sistemas considerados pela entidade como fora do escopo para o DSS PCI, aproveitando esses sistemas para obter acesso a mais sistemas, o que eventualmente fornece um caminho para os sistemas onde os dados do CHD podem ser encontrados. Embora a segmentação possa ajudar a reduzir o número de pontos de exposição para o ambiente de dados do portador do cartão (CDE), isso não é uma solução milagrosa; a implementação da segmentação não substitui uma abordagem holística para garantir a infraestrutura de uma organização.

1.1 Uso pretendido e público-alvo

Esta orientação destina-se a qualquer entidade que procure entender os princípios de escopo e segmentação ao aplicar o DSS PCI ao seu ambiente. As recomendações fornecidas neste documento podem ser usadas por entidades grandes e pequenas para avaliar quais componentes do sistema devem ser cobertos pelos requisitos do DSS PCI. A orientação não aborda a conformidade com o DSS PCI. As entidades devem entrar em contato diretamente com o seu adquirente (banco comercial) ou com a marca do cartão de pagamento, conforme aplicável, para obter informações sobre os programas de conformidade do DSS PCI.

Esta orientação também fornece um método para facilitar discussões de escopo eficazes entre entidades, sendo útil para:

- Comerciantes, adquirentes, emissores, prestadores de serviços, por exemplo, processadores de emissor e prestadores de serviços de token (TSPs), e outros responsáveis por atender aos requisitos do DSS PCI para suas empresas
- Avaliadores (como assessores de segurança qualificados ou assessores internos de segurança) responsáveis por realizar as avaliações do DSS PCI
- Adquirentes que avaliam os relatórios do DSS PCI dos comerciantes ou prestadores de serviços sobre conformidade ou questionários de autoavaliação

- Investigadores forenses PCI (PFIs) responsáveis por determinar o escopo do DSS PCI como parte de uma investigação.

Esta orientação destina-se a ser usada como suplemento ao DSS PCI, mas não se sobrepõe nem substitui os requisitos do DSS PCI. Este documento esclarece os princípios de escopo e fornece orientação que pode ser aplicada a diversas situações.

1.2 Terminologia

Os seguintes termos e abreviações são usados ao longo deste documento:

- CDE - Ambiente de dados do titular do cartão
- CDE - Ambiente de dados do titular do cartão
- SAD - Dados de autenticação confidenciais
- Dados contábeis - Dados do titular do cartão e/ou dados de autenticação confidenciais

As definições destes termos são fornecidas no *Glossário de termos, abreviações e acrônimos do DSS PCI e DSS PA*.

Por fim, cada entidade é responsável por tomar suas próprias decisões de escopo do DSS PCI, projetando segmentação eficaz (se usada) e assegurando que sua própria conformidade com o DSS PCI e requisitos de validação relacionados sejam atendidos. Seguir esta orientação não garante que a segmentação eficaz foi implementada nem garante conformidade com o DSS PCI.

2 Compreensão do escopo e da segmentação do DSS PCI

Em um alto nível, o escopo envolve a identificação de pessoas, processos e tecnologias que interagem com ou poderiam afetar a segurança do CHD. A segmentação envolve a implementação de controles adicionais para separar sistemas com diferentes necessidades de segurança. Por exemplo, para reduzir o número de sistemas no escopo do DSS PCI, a segmentação pode ser usada para manter sistemas dentro do escopo separados de sistemas fora do escopo. A segmentação pode consistir em controles lógicos, controles físicos ou uma combinação de ambos. Exemplos de métodos de segmentação comumente usados para fins de redução do escopo do DSS PCI incluem firewalls e configurações de roteador para evitar que o tráfego passe entre redes fora do escopo e o CDE, configurações de rede que impedem comunicações entre diferentes sistemas e/ou sub-redes e controles de acesso físico.

Os tipos de tecnologias usados para segmentação são frequentemente também usados para gerenciar o acesso entre sistemas ou redes no escopo. Por exemplo:

Para atender ao Requisito 1.2.1 do DSS PCI, uma entidade pode instalar um firewall de rede entre o CDE e a rede corporativa para garantir que apenas sistemas designados na rede corporativa possam se comunicar, através de portas aprovadas, com sistemas no CDE. Além disso, a entidade pode usar o mesmo firewall ou outro firewall para bloquear todas as conexões e impedir o acesso entre o CDE e uma rede fora do escopo. Desta forma, um firewall está sendo usado para implementar um requisito do DSS PCI para sistemas e rede no escopo, e também é usado para segmentar uma rede fora do escopo.

Observe que quando as tecnologias são usadas para gerenciar o acesso entre sistemas e redes para fins de atender aos requisitos do DSS PCI, isso não é considerado segmentação que reduz o escopo do DSS PCI. Ainda no escopo para o DSS PCI, essas comunicações são potencialmente mais seguras do que canais de comunicação não controlados.

Os princípios de escopo e segmentação estão descritos na seção “Escopo de requisitos do DSS PCI” do DSS PCI. Alguns trechos desta seção são fornecidos abaixo com orientação adicional.

Escopo dos requisitos do DSS PCI

Os requisitos de segurança do DSS PCI se aplicam a todos os componentes do sistema que estejam incluídos no ou conectados ao ambiente dos dados do titular do cartão. O ambiente dos dados do titular do cartão (CDE) compreende pessoas, processos e tecnologias que armazenam, processam ou transmitem os dados do titular do cartão ou dados de autenticação confidenciais.¹

O CDE de uma organização é apenas o ponto de partida para determinar o escopo geral do DSS PCI. O escopo preciso do DSS PCI envolve avaliar criticamente os fluxos de CDE e CHD, bem como todos os componentes do sistema conectados e de suporte, para determinar a cobertura necessária para os requisitos do DSS PCI. Sistemas com conectividade ou acesso a ou partir do CDE são considerados sistemas “conectados”. Esses sistemas têm um caminho de comunicação para um ou mais componentes do sistema no CDE. A conectividade pode ocorrer em várias tecnologias, incluindo física, sem fio e virtualizada.

- A conectividade física pode ser através de uma rede tradicional (por exemplo, Ethernet ou comunicação de linha elétrica) ou conexão direta de sistema para sistema (por exemplo, USB, componente, etc.).

¹ DSS PCI v3.2, página 10

- A conectividade sem fio usa diferentes ondas de rádio e frequências como mecanismo de transporte (por exemplo, LANs sem fio, GPRS, Bluetooth e tecnologias celulares). Tecnologias sem fio são frequentemente conectadas a uma rede física.
- A conectividade virtualizada inclui o uso de redes virtuais, máquinas virtuais, firewalls virtuais, switches virtuais, etc. Os dispositivos virtuais normalmente compartilham recursos comuns, como um sistema host subjacente e/ou hipervisor, que podem ser usados para conectar uma partição lógica a outra.

A implementação dessas tecnologias pode ser muito complexa. Portanto, é fundamental que alguém que entenda a tecnologia em uso avalie o impacto dessas tecnologias no escopo.

É importante entender os riscos e impactos se os componentes conectados ao sistema forem excluídos ou ignorados no escopo do DSS PCI. Compromissos de componentes conectados ao sistema geralmente levam ao comprometimento do CDE e ao roubo de CHD.

Os seguintes conceitos de escopo sempre se aplicam:

- Os sistemas localizados dentro do CDE estão no escopo, independentemente da sua funcionalidade ou do motivo pelo qual estão no CDE.
- Da mesma forma, os sistemas que se conectam a um sistema no CDE estão no escopo, independentemente de sua funcionalidade ou do motivo pelo qual eles têm conectividade com o CDE.
- Em uma rede plana, todos os sistemas estão no escopo se qualquer sistema único armazenar, processar ou transmitir dados de conta.

Observe que redes públicas não confiáveis (por exemplo, a internet) não estão no escopo para o DSS PCI. No entanto, os requisitos do DSS PCI devem ser implementados para proteger os sistemas e os dados do escopo da entidade contra redes não confiáveis.

Segmentação da rede

A segmentação da rede ou o isolamento (separação) do ambiente dos dados do titular do cartão do restante da rede corporativa não é um requisito do DSS PCI. Entretanto, ela é recomendada como um método que pode reduzir:

- *O escopo da avaliação do DSS PCI*
- *O custo da avaliação do DSS PCI*
- *O custo e a dificuldade de implementar e manter controles do DSS PCI*
- *O risco de uma organização (reduzido pela consolidação dos dados do titular do cartão em menos locais e mais controlados)*

Sem a segmentação adequada da rede (às vezes chamada de “rede plana”), toda a rede está no escopo da avaliação do DSS PCI.²

A intenção da segmentação é evitar que sistemas fora do escopo sejam capazes de se comunicar com sistemas no CDE ou afetar a segurança do CDE. A segmentação é normalmente obtida por tecnologias e controles de processo que impõem a separação entre os sistemas do CDE e fora do escopo. Quando implementado adequadamente, um componente de sistema segmentado (fora do escopo) não pode afetar a segurança do CDE, mesmo que um invasor tenha obtido acesso administrativo nesse sistema fora do escopo.

² DSS PCI v3.2, página 10

Observe que a conectividade ou acesso é permitido no CDE a partir de sistemas externos ao CDE. No entanto, toda essa conectividade está no escopo para o DSS PCI e todos os requisitos relevantes do DSS PCI se aplicam para garantir essa conexão ou acesso.

A existência de segmentos de rede separados não cria automaticamente a segmentação do DSS PCI. A segmentação é alcançada por meio de controles construídos para fins específicos que criam e aplicam especificamente a separação e para evitar que comprometimentos originários da(s) rede(s) fora do escopo alcancem o CHD.

É importante observar que não há solução ou tecnologia que elimine todos os requisitos do DSS PCI. Ferramentas e tecnologias (como encriptação ou tokenização) podem ajudar a reduzir o risco, reduzir a aplicabilidade de alguns requisitos do DSS PCI, reduzir o tamanho do CDE ou ajudar a atender aos requisitos do DSS PCI com mais facilidade.

Para ajudar a manter a segurança contínua, tais tecnologias devem ser implementadas adequadamente com configurações e processos de configuração específicos para garantir o gerenciamento seguro contínuo da tecnologia. Esses controles devem fazer parte da verificação e dos testes anuais para confirmar que estão operando de forma eficaz.

2.1 Prestadores de serviços e outros terceiros

Além de incluir sistemas internos e redes no escopo, todas as conexões de entidades de terceiros, por exemplo, parceiros de negócios, entidades que prestam serviços de suporte remoto e outros prestadores de serviços, precisam ser identificadas para determinar a inclusão para o escopo do DSS PCI. Assim que as conexões no escopo tiverem sido identificadas, os controles aplicáveis do DSS PCI devem ser implementados para reduzir o risco de uma conexão de terceiros ser usada para comprometer o CDE de uma entidade.

Da mesma forma, se uma entidade terceirizar funções ou instalações no escopo ou utilizar um serviço de terceiros que afete a forma como ela atende aos requisitos do DSS PCI, a entidade precisará trabalhar com o terceiro para garantir que os aspectos aplicáveis do serviço sejam incluídos no escopo para o DSS PCI, seja para a entidade ou para o prestador de serviços. Também é importante que ambas as partes entendam claramente quais requisitos do DSS PCI estão sendo fornecidos pelo prestador de serviços e quais são a responsabilidade da entidade usando o serviço. Consulte o Requisito 12.8 do DSS PCI.

Consulte as *Informações complementares do SSC PCI: Garantia de segurança de terceiros*³ para obter orientação sobre o gerenciamento de relações com terceiros.

2.2 Responsabilidade pela confirmação do escopo

É importante entender a natureza compartilhada da confirmação de que o escopo do DSS PCI foi definido com precisão. O DSS PCI fornece a seguinte orientação:

A entidade é responsável por garantir que seu escopo seja sempre preciso.

Ao menos anualmente e antes da avaliação anual, a entidade avaliada deve confirmar a precisão do seu escopo do DSS PCI identificando todos os locais e fluxos de dados do titular do cartão, bem como identificar todos os sistemas aos quais está conectada ou, se comprometidos, que poderiam afetar o CDE (por exemplo, servidores de autenticação), para garantir que estejam incluídos no escopo do DSS PCI.

A entidade retém a documentação que mostra como o escopo do DSS PCI foi determinado. A documentação é retida para a revisão da assessoria e/ou para referência durante a próxima atividade anual de confirmação do escopo do

³ Disponível no site do SSC PCI: https://www.pcisecuritystandards.org/document_library

DSS PCI. Para cada avaliação do DSS PCI, é necessário que o assessor valide que o escopo da avaliação está corretamente definido e documentado.⁴

Isso significa que, embora a entidade avaliada seja responsável por determinar anualmente o escopo do DSS PCI e confirmar sua precisão, o avaliador que executa a validação do DSS PCI é responsável por confirmar que o escopo foi definido e documentado adequadamente. O avaliador deve questionar as decisões de escopo, se alguma não estiver clara na documentação da entidade avaliada. Nesses casos, o avaliador deve trabalhar em colaboração com a entidade para entender as decisões de escopo tomadas.

Se a segmentação da rede tiver sido implementada e estiver sendo usada para reduzir o escopo da avaliação do DSS PCI, o assessor deverá verificar se a segmentação é adequada para diminuir o escopo da avaliação.⁵

Todos os controles de segmentação também devem ser testados em relação à penetração pelo menos anualmente de acordo com o Requisito 11.3.4 do DSS PCI⁶ para garantir que os controles implementados continuem fornecendo segmentação eficaz.

⁴ DSS PCI v3.2, página 10

⁵ DSS PCI v3.2, página 11

⁶ A partir de 1º de fevereiro de 2018, os prestadores de serviços devem realizar testes de penetração pelo menos a cada seis meses para verificar os controles de segmentação.

3 Definição de escopo e categorias

No *Glossário de termos, abreviações e acrônimos do DSS PCI e PA-DSS*, o escopo é definido como: “Processo de identificação de todos os componentes do sistema, pessoas e processos a serem incluídos na avaliação do DSS PCI. A primeira etapa de uma avaliação do DSS PCI é determinar precisamente o escopo da revisão.”

A definição precisa do escopo envolve avaliar criticamente os componentes do CDE e do sistema conectado para determinar a cobertura necessária para os requisitos do DSS PCI.

Um exercício típico de escopo pode incluir o seguinte:

Atividade	Descrição
Identificar como e onde a organização recebe o CHD.	1. Identificar todos os canais de pagamento e métodos para aceitar o CHD, desde o ponto em que o CHD é recebido até o ponto de destruição, descarte ou transferência.
Localizar e documentar onde os dados da conta são armazenados, processados e transmitidos.	2. Documentar todos os fluxos do CHD e identificar pessoas, processos e tecnologias envolvidas no armazenamento, processamento e/ou transmissão do CHD. Essas pessoas, processos e tecnologias fazem parte do CDE ⁷ .
Identificar todos os outros componentes, processos e funcionários do sistema que estão no escopo.	3. Identificar todos os processos (empresariais e técnicos), componentes e funcionários do sistema com a capacidade de interagir ou influenciar o CDE (conforme identificado no item 2 acima). Essas pessoas, processos e tecnologias estão todos no escopo, pois têm conectividade com o CDE ou poderiam afetar a segurança do CHD de outra forma.
Implementar controles para minimizar o escopo dos componentes, processos e funcionários necessários.	4. Implementar controles para limitar a conectividade entre CDE e outros sistemas no escopo apenas para aquilo que é necessário. 5. Implementar controles para segmentar o CDE de pessoas, processos e tecnologias que não precisam interagir com ou influenciar o CDE.
Implementar todos os requisitos aplicáveis do DSS PCI.	6. Identificar e implementar os requisitos do DSS PCI conforme aplicável aos componentes, processos e funcionários do sistema no escopo.
Manter e monitorar.	7. Implementar processos para garantir que os controles do DSS PCI permaneçam efetivos dia após dia. 8. Garanta que as pessoas, processos e tecnologias incluídas no escopo sejam identificados com precisão quando forem feitas alterações.

⁷ Embora as pessoas que participam do armazenamento, processamento ou transmissão de dados do portador do cartão façam parte do CDE, ao implementar a segmentação para a definição do escopo para o DSS PCI, essas pessoas não precisam ser segmentadas ou isoladas de pessoas que estão fora do CDE. Isso ocorre porque os processos e as tecnologias para implementar e manter a segmentação também garantem que as pessoas no CDE sejam as únicas com o acesso necessário.

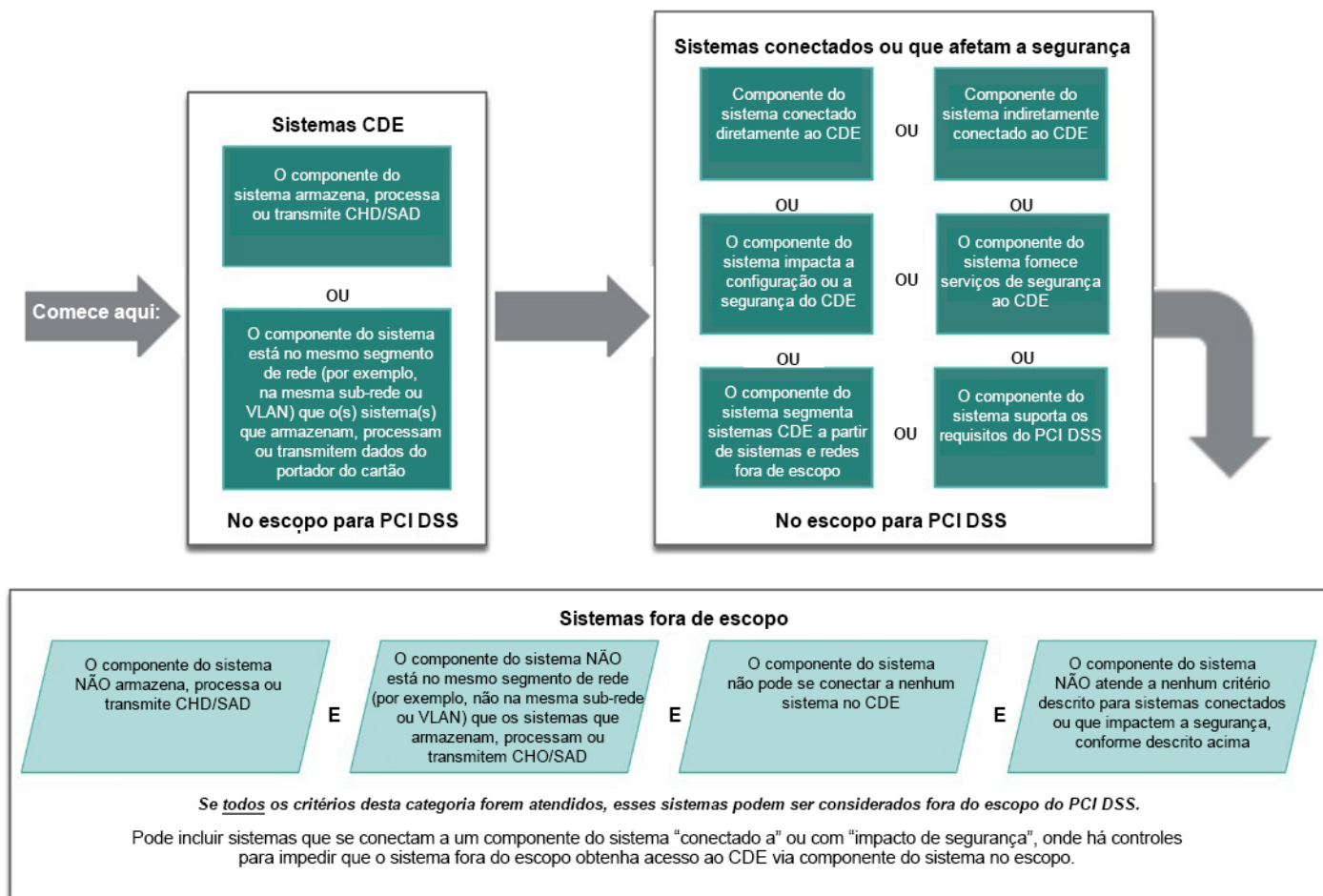
Observe que estar no escopo não significa que todos os requisitos do DSS PCI se aplicam a um determinado componente do sistema; os requisitos do DSS PCI⁸ aplicáveis dependem da função e/ou localização do componente do sistema.

O diagrama e a tabela nesta seção ilustram como os componentes do sistema podem ser categorizados usando vários fatores:

- Se os dados da conta (CHD/SAD) estão sendo armazenados, processados ou transmitidos.
- A conectividade entre o componente do sistema e o CDE.
- Se um componente do sistema afeta a segurança do CDE.

As categorias fornecidas aqui são apenas exemplos e ilustram uma forma de considerar diferentes componentes e o impacto no escopo do DSS PCI. As entidades podem seguir essa abordagem ou usar outro processo de avaliação a seu critério. O uso dessas categorias não é obrigatório.

FIGURA 1 – Categorias de escopo do DSS PCI



Nesta abordagem, os componentes do sistema podem ser categorizados em *apenas uma* dessas categorias. Essas categorias

⁸ As entidades elegíveis para SAQ que atendem a todos os critérios de um SAQ específico podem considerar os requisitos aplicáveis como aqueles identificados dentro daquele SAQ.

são hierárquicas, com sistemas do CDE como a categoria mais alta que deve ser considerada primeiro; se um sistema atender a qualquer critério nos sistemas do CDE, ele será um sistema CDE independentemente de também atender a uma descrição de uma categoria inferior. A próxima categoria inclui sistemas conectados ou que afetam a segurança; esta categoria tem prioridade e é avaliada antes da categoria de sistemas fora do escopo ser considerada. Para ser considerado fora do escopo, um sistema deve atender a TODOS os critérios da categoria fora do escopo e a NENHUM dos critérios de uma categoria mais alta.

A tabela a seguir contém mais detalhes sobre cada categoria:

Tipo de sistema	Descrição	Escopo e aplicabilidade
CDE Sistemas	<ul style="list-style-type: none"> O componente do sistema armazena, processa ou transmite CHD/SAD. OU <ul style="list-style-type: none"> O componente do sistema está no mesmo segmento de rede, por exemplo, na mesma sub-rede ou VLAN que os sistemas que armazenam, processam ou transmitem CHD/SAD. 	Estes sistemas: <ul style="list-style-type: none"> Estão no escopo para o DSS PCI. Devem ser avaliados para determinar a aplicabilidade de cada requisito do DSS PCI⁹.
Sistemas de impacto conectados e/ou de segurança	<ul style="list-style-type: none"> O componente do sistema está em uma rede diferente (ou sub-rede ou VLAN), mas pode se conectar ou acessar o CDE (por exemplo, através de conectividade de rede interna). OU <ul style="list-style-type: none"> O componente do sistema pode se conectar ou acessar o CDE por meio de outro sistema, por exemplo, através de conexão a um jump server que fornece acesso ao CDE. OU <ul style="list-style-type: none"> O componente do sistema pode afetar a configuração ou a segurança do CDE ou como o CHD/SAD é tratado, por exemplo, um servidor de redirecionamento da web ou servidor de resolução de nome. OU <ul style="list-style-type: none"> O componente do sistema fornece serviços de segurança ao CDE, por exemplo, filtragem de tráfego de rede, distribuição de patches ou gerenciamento de autenticação. OU <ul style="list-style-type: none"> O componente do sistema suporta os requisitos do DSS PCI, como servidores de tempo e servidores de armazenamento de registros de auditoria. OU <ul style="list-style-type: none"> O componente do sistema fornece segmentação do CDE de sistemas e redes fora do escopo, por exemplo, firewalls configurados para bloquear o tráfego de redes não confiáveis. 	Estes sistemas: <ul style="list-style-type: none"> Estão no escopo para o DSS PCI. Mesmo quando uma conexão é limitada a portas ou serviços específicos em sistemas específicos, esses sistemas estão incluídos no escopo para verificar se os controles de segurança aplicáveis estão em vigor. Devem ser avaliados para determinar a aplicabilidade de cada requisito do DSS PCI⁹. Não devem fornecer um caminho de acesso entre sistemas do CDE e sistemas fora do escopo.

⁹ As entidades elegíveis para SAQ que atendem a todos os critérios de um SAQ específico podem considerar os requisitos aplicáveis como aqueles identificados dentro daquele SAQ.

Tipo de sistema	Descrição	Escopo e aplicabilidade
Sistemas fora do escopo	<ul style="list-style-type: none"> • O componente do sistema NÃO armazena, processa ou transmite CHD/SAD. <p>E</p> <ul style="list-style-type: none"> • O componente do sistema NÃO está no mesmo segmento de rede ou na mesma sub-rede ou VLAN que os sistemas que armazenam, processam ou transmitem CHD. <p>E</p> <ul style="list-style-type: none"> • O componente do sistema não pode se conectar ou acessar qualquer sistema no CDE. <p>E</p> <ul style="list-style-type: none"> • O componente do sistema não pode obter acesso ao CDE nem afetar um controle de segurança para CDE por meio de um sistema no escopo. <p>E</p> <ul style="list-style-type: none"> • O componente do sistema não atende a nenhum critério descrito para sistemas conectados ou que afetam a segurança, conforme acima. <p>Observação: Esses sistemas não estão no escopo para o DSS PCI, mas ainda podem representar um risco para o CDE se não estiverem seguros. Recomenda-se fortemente que as melhores práticas de segurança sejam implementadas para todos os sistemas/redes fora do escopo.</p>	Sistemas fora do escopo: <ul style="list-style-type: none"> • Não estão no escopo para o DSS PCI, portanto, os controles do DSS PCI não são necessários. • Não têm acesso a nenhum sistema do CDE; se houver algum acesso, o sistema está no escopo. • São considerados não confiáveis (ou “públicos”); não há garantia de que foram devidamente protegidos. • Se estiverem na mesma rede (ou sub-rede ou VLAN) ou de outra forma tiverem conectividade a um sistema conectado ou que afeta a segurança, deve haver controles para impedir que o sistema fora do escopo obtenha acesso ao CDE através dos sistemas no escopo. Esses controles devem ser validados pelo menos anualmente.

3.1 Verificação da segmentação de sistemas fora do escopo

Para ser considerado fora do escopo, um componente do sistema não deve ter acesso a nenhum sistema no CDE. É possível que um sistema fora do escopo esteja no mesmo segmento de rede ou sub-rede como um sistema conectado ou que afeta a segurança, desde que o sistema fora do escopo não possa acessar o CDE, seja através do sistema no escopo ou por meio de qualquer outro método.

Para que um sistema seja considerado fora do escopo, os controles devem estar em vigor para fornecer uma garantia razoável de que o sistema fora do escopo não pode ser usado para comprometer um componente do sistema no escopo, pois o sistema no escopo poderia ser usado para obter acesso ao CDE ou afetar a segurança do CDE. Exemplos de controles que podem ser aplicados para evitar que sistemas fora do escopo comprometam um sistema conectado ou que afeta a segurança incluem:

- Firewall baseado em host e/ou sistema de detecção e prevenção de intrusão (IDS/IPS) em sistemas no escopo que bloqueiam tentativas de conexão de sistemas fora do escopo.
- Controles de acesso físico que permitem que apenas usuários designados acessem sistemas no escopo.
- Controles de acesso lógico que permitem que apenas usuários designados façam login em sistemas no escopo.
- Autenticação de múltiplos fatores em sistemas no escopo.
- Restringir privilégios de acesso administrativo a usuários e sistemas/redes designados.
- Monitorar ativamente comportamentos suspeitos de rede ou sistema que possam indicar um sistema fora do escopo tentando obter acesso a um componente do sistema no escopo ou ao CDE.

Esses exemplos não são completos, nem seriam aplicáveis a todos os cenários. A intenção de tais controles é fornecer uma garantia razoável de que um sistema fora do escopo não possa alavancar um componente do sistema no escopo para obter acesso ao CDE ou afetar a segurança do CDE. Os controles usados para fornecer essa garantia fazem parte da verificação geral da segmentação. Assim que todos os controles de segmentação forem verificados, os sistemas podem ser considerados fora do escopo para o DSS PCI.

Segurança de sistemas e redes fora do escopo

Embora não seja necessário implementar controles do DSS PCI em sistemas fora do escopo, é altamente recomendável como melhor prática evitar que sistemas fora do escopo sejam usados para fins maliciosos. Exemplos de controles que podem ajudar a reduzir esse risco incluem minimizar o acesso entre sistemas fora do escopo e redes públicas para apenas o que é necessário, mantendo os sistemas atualizados com patches de segurança e software antivírus usando mecanismos de detecção de mudança (por exemplo, software de monitoramento de integridade de arquivos) e implementação de controles de acesso com base em autenticação forte e menor privilégio.

Observação: Proteger sistemas/redes fora do escopo não os leva ao escopo dos requisitos do DSS PCI. Entretanto, se esses controles também impedem que os sistemas fora do escopo acessem o CDE, os controles devem ser incluídos na verificação da segmentação.

4 Exemplo de implementações de segmentação: Serviços compartilhados

Os exemplos nesta seção ilustram apenas dois tipos de cenários; há muitas outras opções de implementação e configuração que podem ser aplicadas para segmentar o CDE de sistemas fora do escopo. Determinada implementação não precisa atender aos critérios conforme declarado nestes exemplos. Uma implementação pode precisar de mais ou menos controles dependendo do ambiente específico. Como todos os ambientes e organizações são diferentes, esses exemplos são simplificados para fornecer clareza em torno da questão dos limites do escopo.

Os exemplos a seguir não abordam o risco de um invasor comprometer ou obter acesso a uma conta de administrador na rede fora do escopo e depois usar essa conta para obter acesso ao CDE. Para mitigar o risco de tais ataques, a capacidade de usar contas de administrador e usuário deve ser limitada ao(s) sistema(s) e/ou segmento(s) de rede para o(s) qual(is) o pessoal administrador tem uma função administrativa específica atribuída. Dessa maneira, uma conta comprometida em uma rede fora do escopo não pode ser aproveitada para obter acesso a outros sistemas, redes ou ao CDE.

Para a segmentação de sistemas fora do escopo ser eficaz, controles rigorosos devem estar em vigor para monitorar e aplicar a separação. O registro diligente e o monitoramento de eventos é essencial para detectar e responder a falhas nos controles de segmentação que podem resultar em acesso não autorizado ao CDE da rede fora do escopo.

Os seguintes princípios se aplicam ao Exemplo 1 (descrito na Seção 5.1) e ao Exemplo 2 (Seção 5.2):

- Três zonas de rede distintas são definidas:
 - LAN corporativa
 - Serviços compartilhados
 - CDE
- As regras de firewall e roteador garantem que:
 - As únicas conexões permitidas dentro e fora do CDE são com os Serviços compartilhados, através de portas e sistemas especificamente designados, e somente quando houver uma necessidade comercial documentada.
 - Todas as tentativas de conexão entre a LAN corporativa e o CDE estão ativamente bloqueadas (nenhum tráfego originado na LAN corporativa é permitido no CDE).
 - Comunicações entre Serviços compartilhados e a LAN corporativa:
 - São permitidas apenas entre sistemas designados, portas, serviços etc., e todas as outras tentativas de conexão são bloqueadas.
 - São limitadas pela necessidade comercial, por exemplo, a conectividade entre estações de trabalho e um Servidor de diretório é limitada apenas ao tráfego de autenticação de rede.
- O CHD não é armazenado, processado ou transmitido fora do CDE, exceto através de conexões de rede seguras com o banco/processador adquirente (não mostrado nos diagramas).
- Todos os requisitos relevantes do DSS PCI são aplicados:
 - Às redes do CDE e de serviços compartilhados e aos componentes do sistema
 - Ao gerenciamento e à garantia de conectividade entre o CDE e os Serviços compartilhados, incluindo firewalls, ACLs, IDS/IPS, antimalware e outras ferramentas e técnicas de defesa contra ameaças
 - Ao gerenciamento e à garantia do tráfego de entrada/saída entre os Serviços compartilhados e a LAN corporativa.

- O acesso físico à rede do CDE e de Serviços compartilhados é restrito a funcionários especificamente designados, conforme definido pela necessidade empresarial.
- Todos os controles que estabelecem segmentação estão incluídos em cada avaliação do DSS PCI para validar sua eficácia, incluindo aqueles que limitam as conexões a portas ou serviços específicos em sistemas específicos.
- O tráfego e a atividade entre os Serviços compartilhados e o CDE, e dentro do CDE, são ativamente monitorados e inspecionados para detectar anomalias e reduzir o risco de um comprometimento dos Serviços compartilhados levando a um comprometimento do CDE.

4.1 Exemplo 1: Serviços compartilhados “conectados”

Observação: Este exemplo e os diagramas relacionados são apenas para fins ilustrativos. Cada rede é diferente e as técnicas de segmentação que funcionam bem em uma rede podem não funcionar em outra rede. Assim, qualquer método de segmentação usado deve ser completamente testado de acordo com os requisitos do DSS PCI para confirmar que funciona como esperado e continua fornecendo segmentação eficaz nesse ambiente. Da mesma forma, os controles observados neste documento

“Serviços compartilhados” são componentes comuns do sistema que fornecem serviços, como suporte de autenticação ou gerenciamento, aos componentes do sistema em toda a empresa da organização, incluindo sistemas do CDE e sistemas fora do escopo.

Serviços comuns compartilhados incluem, entre outros:

- Diretório e autenticação (por exemplo, Active Directory, LDAP/AAA)
- NTP – Network Time Protocol (Protocolo de tempo de rede)
- DNS – Domain Name Service (Serviço de nome de domínio)
- SMTP – Simple Mail Transfer Protocol (Protocolo simples de transferência de correspondência)
- Ferramentas de monitoramento e digitalização
- Ferramentas de backup
- Servidores de implantação de antivírus e patch

Para este exemplo, os Serviços compartilhados estão localizados fora de um CDE segmentado, mas fornecem serviços ao CDE. Os Serviços compartilhados também fornecem autenticação e/ou outras funções de suporte operacional a outros sistemas corporativos considerados fora do escopo. Como esses Serviços compartilhados estão se conectando ao e fornecendo serviços no CDE, eles estão no escopo do DSS PCI.

A pergunta neste cenário é como implementar a segmentação de modo que os sistemas na LAN corporativa possam se conectar aos Serviços compartilhados, mas sejam segmentados de forma eficaz a partir do CDE de modo que eles não possam acessar o CDE. Em outras palavras, como estabelecer Serviços compartilhados que suportam tanto o CDE quanto a LAN corporativa, ao mesmo tempo mantendo os sistemas na LAN corporativa fora do escopo do DSS PCI.

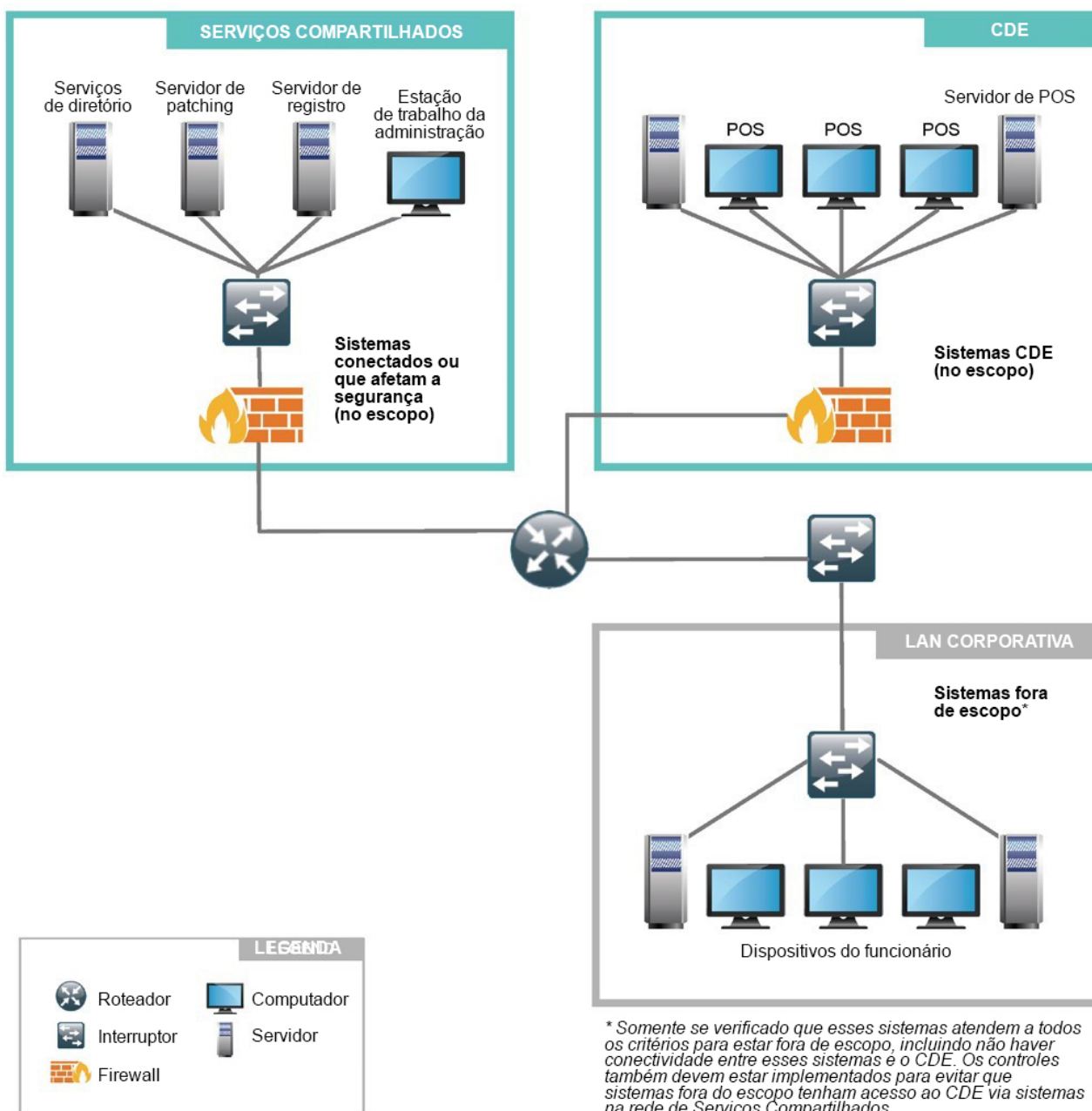
Os princípios a seguir aplicam-se adicionalmente àqueles definidos acima. Consulte as Figuras 2 e 3.

- O acesso administrativo aos sistemas de Serviços compartilhados é permitido apenas a partir da rede de Serviços compartilhados, e todos esses acessos são registrados e monitorados.
- O acesso administrativo aos sistemas do CDE é permitido apenas a partir de sistemas no CDE ou de sistemas designados na rede de Serviços compartilhados.

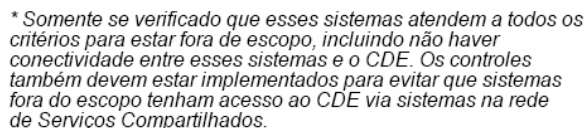
- A autenticação de múltiplos fatores é usada para todo acesso administrativo a partir dos sistemas de Serviços compartilhados ao CDE. Todo acesso administrativo ao CDE é registrado e monitorado.
- Contas usadas para acessar Serviços compartilhados da LAN corporativa não têm acesso ao CDE.
- Todos os controles de acesso são estabelecidos e gerenciados nos firewalls nas zonas de Serviços compartilhados e CDE.

**FIGURA 2 – Exemplo de ilustração de segmentação:
Serviços compartilhados “conectados”**

Cenário 1



Cenário 1: Fluxo de dados lógicos



A tabela a seguir resume as zonas de rede ilustradas nas Figuras 2 e 3 acima, e o impacto potencial no escopo do DSS PCI.

Zonas de rede	Categoria	Impacto no escopo do DSS PCI
CDE	Sistemas do CDE	Totalmente no escopo para todos os requisitos aplicáveis do DSS PCI
Serviços compartilhados	Sistemas conectados e/ou que afetam a segurança	Totalmente no escopo para todos os requisitos aplicáveis do DSS PCI
LAN corporativa	Sistemas fora do escopo	<p>Fora do escopo</p> <p><i>Os controles de segmentação devem ser totalmente testados e verificados antes que os sistemas da LAN corporativa possam ser determinados como fora do escopo. Os sistemas e funcionários da LAN corporativa que acessam os Serviços compartilhados não podem obter acesso ao CDE através dos Serviços compartilhados. Os controles de segmentação precisam ser verificados pelo menos anualmente.</i></p>

4.2 Exemplo 2: Estação de trabalho de administração do CDE fora do CDE

Observação: Este exemplo e os diagramas relacionados são apenas para fins ilustrativos. Cada rede é diferente e as técnicas de segmentação que funcionam bem em uma rede podem não funcionar em outra rede. Assim, qualquer método de segmentação usado deve ser completamente testado de acordo com os requisitos do DSS PCI para confirmar que funciona como esperado e continua fornecendo segmentação eficaz nesse ambiente. Da mesma forma, os controles observados neste documento

Um administrador de sistema frequentemente tem responsabilidades em relação aos sistemas em toda a empresa, o que pode incluir sistemas do CDE, sistemas conectados e que afetam a segurança, bem como sistemas fora do escopo. As contas de administrador são contas privilegiadas que precisam ser gerenciadas e monitoradas cuidadosamente, uma vez que indivíduos com esses privilégios mais altos podem conceder privilégios elevados para outros usuários e podem acessar, adicionar, excluir e alterar muitos (se não todos) arquivos e configurações do sistema, alterar ou excluir dados de registro de auditoria e acessar CHD.

Para este exemplo, um administrador de sistema é responsável pelos sistemas do CDE, bem como pelos sistemas em Serviços compartilhados e sistemas fora do escopo na LAN corporativa. A estação de trabalho do administrador está localizada na LAN corporativa e fora do CDE. Portanto, a administração do sistema do CDE origina-se de fora, mas exige conectividade com os dispositivos dentro do CDE.

Este exemplo se baseia na rede de Serviços compartilhados do exemplo anterior, além de:

- 1) Uma estação de trabalho do administrador na LAN corporativa e
- 2) Um jumpbox na rede de Serviços compartilhados para gerenciar e controlar o acesso administrativo no CDE.

A principal questão para este exemplo é como implementar uma segmentação que permite a administração segura de sistemas do CDE a partir de um sistema que afeta a segurança e que está localizado na LAN corporativa, além de também manter o resto dos sistemas da LAN corporativa fora do escopo.

A abordagem adotada neste exemplo é semelhante à de um cenário de acesso remoto, em que um administrador se conecta remotamente ao CDE a partir de sua rede doméstica:

- A LAN corporativa é uma rede não confiável de forma semelhante à rede doméstica.
- A zona de rede de Serviços compartilhados atua como um DMZ, fornecendo serviços tanto para computadores não confiáveis como para um usuário confiável com acesso ao CDE.
- A estação de trabalho do admin é protegida da mesma forma que um computador remoto precisa ser, com software de firewall pessoal, autenticação de múltiplos fatores e todos os outros requisitos aplicáveis do DSS PCI em vigor.
- O acesso ao CDE a partir de redes não confiáveis é gerenciado e controlado por sistemas exclusivos na rede de Serviços compartilhados.

Todos os controles que se aplicam ao Exemplo 1 também se aplicam a este exemplo, com a exceção de que o acesso administrativo ao CDE é permitido a partir de uma estação de trabalho administrativa designada na LAN corporativa. Além dos controles definidos acima, os seguintes princípios de segmentação são aplicáveis a este exemplo. (Consulte as Figuras 4 e 5.)

- Um “jumpbox” (host Bastion¹⁰) está instalado na rede de Serviços compartilhados.
- As regras de firewall e roteador garantem que
 - As conexões com o jump host da LAN corporativa são restritas apenas a funcionários designados da estação de trabalho do admin e todas as outras tentativas de conexão são bloqueadas.
 - A estação de trabalho do admin não pode acessar o CDE diretamente e deve passar pelo Jump Box para todos os acessos ao CDE.
- Ferramentas de monitoramento ativo e prevenção de perda de dados (DLP) estão em vigor para garantir que os dados da conta não possam ser transferidos do CDE para o jumpbox.
- A administração do próprio jumpbox ocorre somente através do console local, e não há gerenciamento remoto deste dispositivo.
- A estação de trabalho do admin não armazena, processa ou transmite o CHD.
- A estação de trabalho do admin está totalmente no escopo para o DSS PCI e todos os requisitos aplicáveis do DSS PCI são aplicados.
- A estação de trabalho do admin (que está essencialmente localizada em uma rede não confiável) é protegida contra a internet através da funcionalidade de firewall pessoal, conforme definido no Requisito 1.4 do DSS PCI.
- O uso da estação de trabalho do admin é restrito aos funcionários administrativos designados.
- O acesso ao jumpbox a partir da estação de trabalho do admin acontece por meio de uma conta de usuário diferente daquela usada para administrar o CDE. A conta usada para acessar o jumpbox não tem privilégios elevados no Jump Box.

¹⁰ Um computador projetado e configurado especificamente para suportar ataques. (Fonte: wikipedia.org)

- O acesso ao jumpbox a partir da estação de trabalho do admin exige a autenticação de múltiplos fatores para indivíduos. Pelo menos um dos métodos de autenticação de múltiplos fatores é independente da estação de trabalho do admin e está “nas mãos” do pessoal de administrador designado (por exemplo, um cartão inteligente físico ou token é usado como autenticação do tipo “algo que você tem”).
- Todos os requisitos aplicáveis do DSS PCI estão em vigor para gerenciar e proteger a conectividade entre a estação de trabalho e o jumpbox do admin, incluindo firewalls, IDS/IPS, anti-malware e outras ferramentas e técnicas de defesa contra ameaças.
- Todos os requisitos aplicáveis do DSS PCI estão em vigor para gerenciar e proteger a conectividade entre o jumpbox e o CDE, incluindo firewalls, IDS/IPS, anti-malware e outras ferramentas e técnicas de defesa contra ameaças.

FIGURA 4 – Exemplo de ilustração de segmentação: Administração de sistemas do CDE a partir de um sistema que afeta a segurança na LAN corporativa

Cenário 1

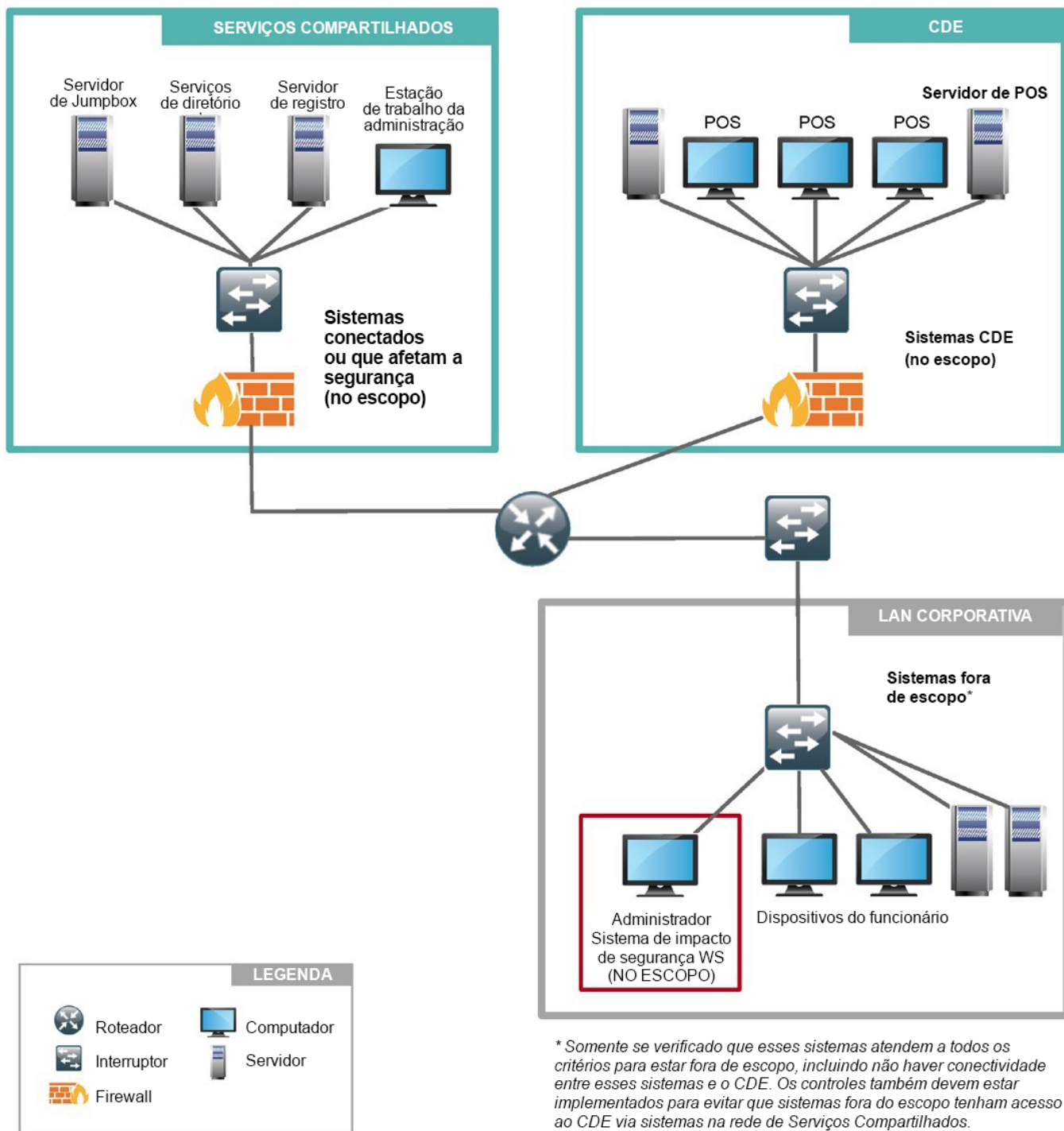
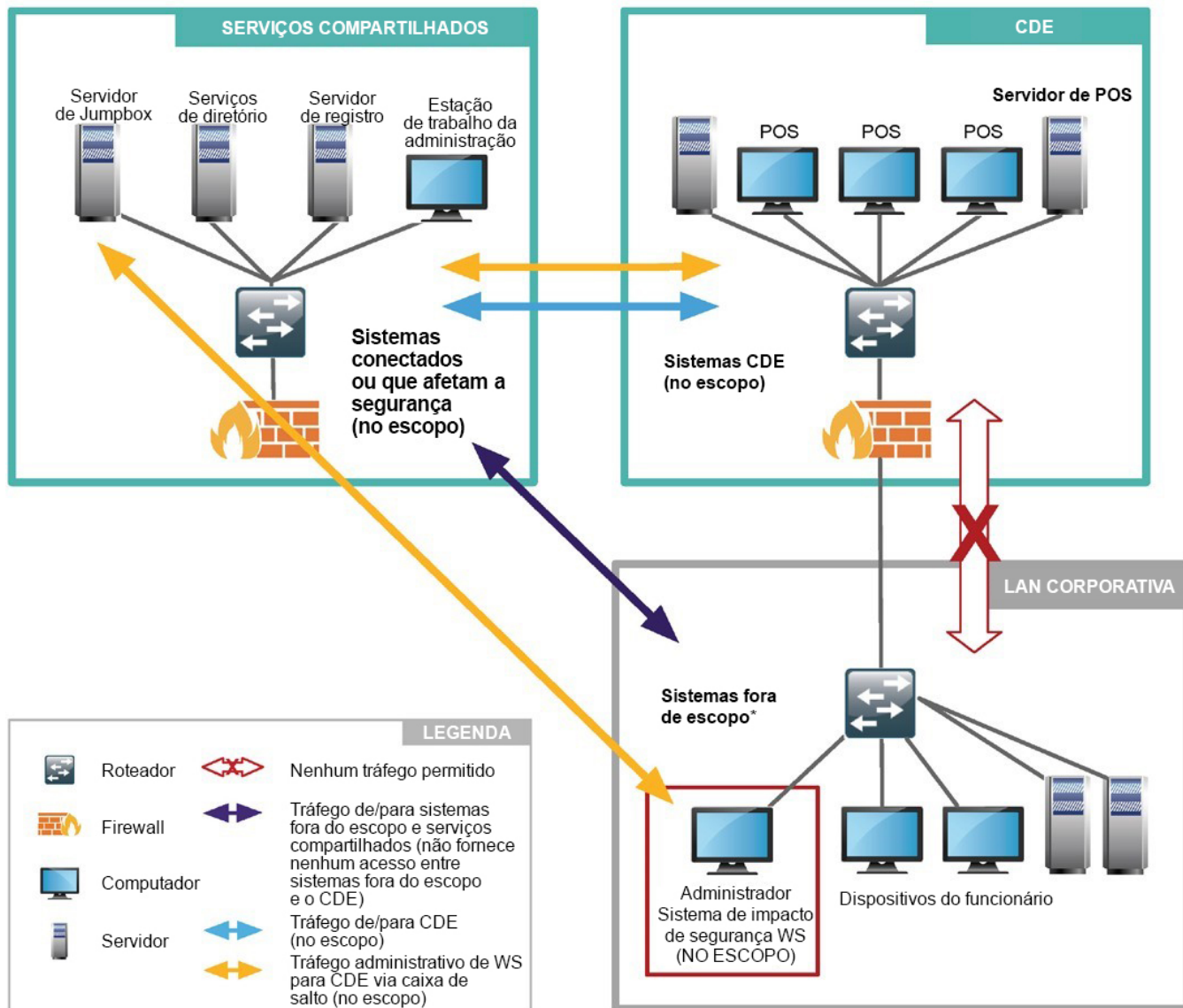


FIGURA 5 – Fluxo de dados lógicos: Administração de sistemas do CDE a partir de um sistema que afeta a segurança na LAN corporativa

Cenário 2: Fluxo de dados lógicos



* Somente se verificado que esses sistemas atendem a todos os critérios para estar fora de escopo, incluindo não haver conectividade entre esses sistemas e o CDE. Os controles também devem estar implementados para evitar que sistemas fora do escopo tenham acesso ao CDE via sistemas na rede de Serviços Compartilhados.

A tabela a seguir resume as zonas de rede ilustradas nas Figuras 4 e 5 acima, e o impacto potencial no escopo do DSS PCI.

Zonas/sistemas de rede	Categoria	Impacto no escopo do DSS PCI
CDE	Sistemas do CDE	Totalmente no escopo para todos os requisitos aplicáveis do DSS PCI
Serviços compartilhados (incluindo Jump Box)	Sistema conectado e/ou que afeta a segurança	Totalmente no escopo para todos os requisitos aplicáveis do DSS PCI
Estação de trabalho admin na LAN corporativa	Sistema que afeta a segurança	Totalmente no escopo para todos os requisitos aplicáveis do DSS PCI
Outros sistemas na LAN corporativa	Sistemas fora do escopo	Fora do escopo <i>Os controles de segmentação devem ser totalmente testados e verificados antes que outros sistemas na LAN corporativa possam ser determinados como fora do escopo. Os sistemas e funcionários da LAN corporativa que acessam os Serviços compartilhados não podem obter acesso ao CDE através dos Serviços compartilhados. Os controles de segmentação precisam ser verificados pelo menos anualmente.</i>

5 Conclusão

Ao definir o escopo de um ambiente para o DSS PCI, é importante começar sempre com a suposição de que tudo está no escopo até que seja verificado que todos os controles necessários estão em vigor e estão realmente fornecendo segmentação eficaz. A segmentação eficaz pode reduzir enormemente o risco de os sistemas do CDE serem afetados por vulnerabilidades de segurança ou comprometimentos originários de sistemas fora do escopo.

Lembre-se de que o escopo inadequado (decidir que algo está fora do escopo sem verificação adequada) pode colocar um negócio em risco. Para ser eficaz, o escopo e a segmentação exigem planejamento, projeto, implementação e monitoramento cuidadosos. Muitos comprometimentos ocorreram por meio de sistemas e redes incorretamente determinados como estando fora do escopo, sendo que a entidade violada confiou na segmentação e descobriu, após a violação, que esses controles não estavam protegendo suas redes com eficácia. Portanto, é fundamental que as entidades se concentrem na segurança de todo o ambiente em vez de apenas no que é exigido pelo DSS PCI para minimizar os riscos às suas organizações.

Sobre o Conselho dos Padrões de Segurança PCI

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