

Conformidade com o padrão de segurança de dados do setor de cartões de crédito e débito

Soluções de acesso corporativo seguro e remoto para os Requisitos 7 e 8 do PCI DSS



O padrão PCI (Payment Card Industry, setor de cartões de crédito e débito) deixa um fato muito claro: é responsabilidade da empresa proteger os dados de titulares de cartão, onde quer que esses dados residam. Esses requisitos vão muito além da proteção do perímetro, e exigem que os bancos, os comerciantes e os processadores de pagamento protejam os dados de cartão em si, assegurem que apenas pessoas autorizadas possam acessar os sistemas de dados de titulares de cartão e garantam que as pessoas que tentam acessar os dados de cartão sejam quem afirmam ser.

Por isso, para os executivos que lidam com a conformidade com o PCI DSS (Data Security Standard, padrão de segurança de dados), é extremamente importante controlar o acesso aos dados de titulares de cartão e proteger as identidades dos indivíduos que acessam os sistemas de dados de titulares de cartão. Na verdade, o Requisito 7 obriga as empresas a “restringir o acesso aos dados de titulares de cartão apenas aos que realmente precisam dos dados”. Ou seja, as marcas de cartão de crédito e débito querem garantir que os comerciantes, bancos e processadores de pagamento assumam a responsabilidade pelo controle de acesso às informações sobre cartões que eles retêm.

Além disso, por meio do Requisito 8, o padrão PCI orienta as empresas a “atribuir uma ID exclusiva a cada pessoa com acesso ao computador”. Para os executivos, no entanto, a intenção não é apenas estabelecer identidades exclusivas: é assegurar que os usuários que acessam a rede e os sistemas de dados de titulares de cartão, tanto interna quanto remotamente, sejam usuários autênticos.

Segurança para dados de cartão de crédito — e mais além

Para os clientes que estão se esforçando para atender ao Requisito 7 do PCI DSS, o software RSA Access Manager oferece uma solução sólida e dimensionável para o controle de acesso aos dados em aplicativos com base na Web. Com o software RSA Access Manager, as empresas podem assegurar que os usuários somente poderão acessar informações confidenciais — como os dados de cartões de crédito e informações sobre parceiros, clientes e funcionários — se receberem direitos exclusivos para tal acesso. O RSA Access Manager permite que os clientes apliquem de modo centralizado o acesso a quaisquer informações essenciais sobre os negócios ou clientes, ajudando a aumentar a segurança ao garantir que sejam implementados controles consistentes de ponto de acesso com base na Web.

À medida que os clientes passarem a adotar a atribuição de identidades rígidas para os usuários, o RSA SecurID fornece os recursos para atender ao Requisito 8, por meio de uma série de tokens de autenticação/autenticadores de dois fatores com base em hardware e software. As RSA Digital Certificate Solutions também estão disponíveis para oferecer aos clientes flexibilidade para escolher o mecanismo de autenticação que melhor atenda às suas necessidades.

Vantagens para o cliente: dados corporativos seguros

Com as soluções RSA para dados corporativos seguros, você terá oportunidade de:

- Proteger efetivamente os dados de cartões de crédito onde quer que estejam em toda empresa e, também, gerenciar essa segurança de modo centralizado.
- Assegurar que sua estratégia de proteção de dados possa ser dimensionada para adaptar-se a mudanças nos negócios e que seus dados essenciais estarão disponíveis e protegidos, independente de onde sejam necessários no ciclo de vida das informações.
- Aproveitar a capacidade de expansão das soluções RSA de dados corporativos seguros para proteger todos os tipos de informações valiosas — sejam sobre os negócios, clientes, parceiros e funcionários — em toda a empresa.

Componentes da solução RSA PCI

- > **RSA Access Manager:** solução RSA para acesso seguro à Web permite que os comerciantes, bancos e processadores de pagamento garantam que apenas os usuários da empresa que realmente precisarem terão acesso aos dados de titulares de cartão em sistemas de PCI com base na Web.
- > **Soluções RSA de dados corporativos seguros:** as soluções RSA de dados corporativos seguros permitem que as empresas afetadas pelo padrão PCI protejam os dados de titulares de cartão em todos os pontos de criptografia e gerenciem de modo centralizado as chaves de criptografia em toda a empresa:
 - RSA Database Security Manager
 - RSA File Security Manager
 - RSA Key Manager
 - CipherOptics IP Security Gateway
 - Dispositivos de segurança de armazenamento Decru DataFort®
 - Dispositivos NeoScale CryptoStor®
- > **RSA enVision:** a solução RSA para gerenciamento de informações de conformidade e segurança permite que as empresas afetadas pelo PCI DSS facilitem o processo de auditoria, estabelecendo um ponto centralizado de controle e monitoramento de acesso aos dados de titulares de cartão em um ambiente inteiro de PCI.
- > **RSA SecurID:** solução RSA para proteção de acesso aos dados corporativos ajuda os clientes a assegurar que os usuários que acessam os sistemas de dados de titulares de cartão, e toda a rede de TI realmente sejam quem afirmam ser.
- > **Serviços profissionais RSA:** : os serviços profissionais RSA oferecem uma ampla variedade de recursos, como ajudar os clientes a se preparar para uma auditoria de PCI DSS, oferecer suporte à detecção ampla de dados de titulares de cartão em toda a empresa e implementar tecnologias para correção de problemas.
- > **EMC Celerra e EMC Centera:** a integração pronta para usar do EMC Celerra e EMC Centera com a tecnologia RSA enVision permite que os clientes armazenem com economia os dados essenciais de registro para auditoria do padrão PCI.

Além das tecnologias que ajudam a cumprir os Requisitos 7 e 8 do PCI DSS, o RSA SecurID pode ser aproveitado para proteger com maior eficiência a infra-estrutura de cartão de crédito e débito de um cliente. Mais especificamente, o programa de parceria RSA Secured oferece integração imediata do RSA SecurID com centenas de sistemas que podem fazer parte da infra-estrutura do padrão PCI (por exemplo, VPNs, firewalls, servidores de aplicativos), permitindo que os clientes garantam a confiabilidade

daqueles que acessam esses sistemas. E enquanto o programa de parceria RSA Secured ajuda a manter a conformidade com o PCI DSS, a autenticação mais rígida dos sistemas de TI ajuda a melhorar a segurança muito além das necessidades de auditoria do PCI DSS.

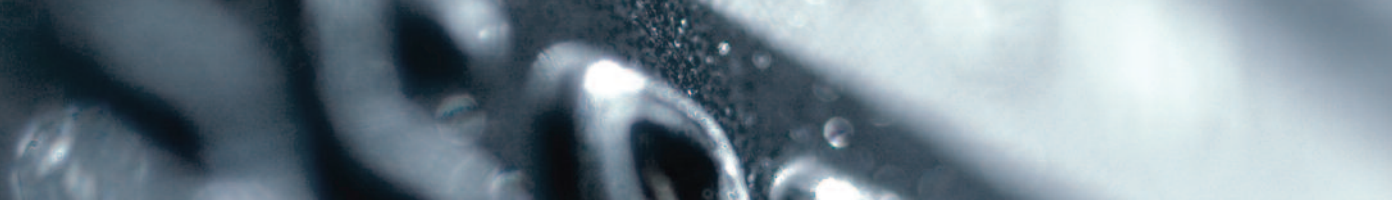
Para obter mais informações sobre as soluções RSA que ajudam os clientes a resolver a conformidade com PCI DSS, visite www.rsa.com/pci

Requisito 7 do PCI DSS: restringir o acesso aos dados do titular do cartão apenas aos que realmente precisam dos dados

Requisito 8 do PCI DSS: atribuir uma ID exclusiva para cada pessoa com acesso ao computador

As soluções RSA para acesso corporativo seguro permitem que os clientes cumpram o requisito 7 do padrão PCI, assegurando que apenas usuários autorizados possam acessar os dados de titulares de cartão em sistemas de PCI com base na Web. Além disso, as soluções RSA para proteção de acesso aos dados corporativos são diretamente alinhadas para oferecer suporte à conformidade com o Requisito 8 do PCI DSS.

Requisito do PCI DSS	Recursos da RSA
Requisito 7.1: limitar o acesso aos recursos de computadores e às informações sobre titulares de cartões apenas às pessoas cuja função exigir tal acesso.	<p>O software RSA Access Manager ajuda os clientes a assegurar que apenas as pessoas autorizadas poderão acessar os dados de titulares de cartão em aplicativos com base na Web. Além disso, esses privilégios podem ser atribuídos com base nas responsabilidades do cargo de uma pessoa ou de um grupo.</p> <p>Os direitos do RSA Access Manager podem ser definidos com base em pessoas ou grupos. Os direitos podem ser definidos por atributos exclusivos, como um cargo (por exemplo, departamento de contabilidade), o que ajuda a assegurar que o acesso seja automaticamente cancelado se, por exemplo, um membro da empresa for transferido para outro departamento.</p> <p>O RSA Access Manager permite que os clientes centralizem o acesso dos dados de titular de cartão com base na Web, ajudando a aumentar a segurança ao garantir que sejam implementados controles consistentes de ponto de acesso com base na Web.</p>
Requisito 7.2: estabelecer um mecanismo para os sistemas com diferentes usuários que restrinja o acesso com base na necessidade para o cargo do usuário e que seja definido para “negar todos” a menos que especificamente permitido.	<p>O software RSA Access Manager oferece a habilidade de restringir o acesso aos dados com base em regras de negócios predefinidas e/ou uma função de usuário dentro da empresa. O software oferece, prontos para uso imediato, recursos para “negar todos”.</p>
Requisito 8.2: além de atribuir uma ID exclusiva, aplicar pelo menos um dos métodos a seguir para autenticar todos os usuários: 1) senha 2) dispositivos de token (por exemplo, SecurID, certificados ou chave pública) 3) biométrica.	<p>O RSA SecurID permite o cumprimento desse requisitos, oferecendo uma série de tokens de autenticação/autenticadores de dois fatores com base em hardware e software. Além disso, as RSA Digital Certificate Solutions oferecem aos clientes flexibilidade para escolher o mecanismo de autenticação que melhor atende às suas necessidades.</p>
Requisito 8.3: implementar autenticação de dois fatores para acesso remoto à rede pelos funcionários, administradores e terceiros. Usar tecnologias como o serviço de autenticação remota e discagem (RADIUS) ou TACACS (Terminal Access Controller Access Control System, sistema de controle de acesso para controlador de acesso a terminal) com tokens; ou VPNs (com base em SSL/TLS ou IPSEC) com certificados específicos.	<p>O RSA SecurID permite que as empresas implementem autenticação de dois fatores por meio de uma série de opções de token para autenticação de dois fatores com base em hardware e software. Além disso, os parceiros RSA Secured oferecem soluções para acesso remoto com integração imediata com o RSA SecurID, tornando mais simples para as empresas adotar processos de autenticação sólida dos usuários que acessam os recursos por conexões VPN.</p>
Requisito 8.4: criptografar todas as senhas durante a transmissão e o armazenamento em todos os componentes do sistema.	<p>O RSA SecurID (mais especificamente, o RSA SID200 PINpad Authenticator and Software Authenticator) permite que o PIN (Personal Identification Number, número de identificação pessoal) do usuário final seja criptografado antes de ser transmitido pela rede. Além disso, toda comunicação realizada entre os agentes do RSA SecurID e o servidor são criptografadas. Por fim, todas as informações do PIN do usuário final são completamente criptografadas durante o armazenamento no servidor.</p>
Requisito 8.5: assegurar o gerenciamento apropriado de autenticação e de senha dos usuários não-consumidores e de administradores em todos os componentes do sistema.	<p>A tecnologia RSA SecurID ajuda seus clientes a exceder esse requisito, oferecendo meios para que realizem autenticação sólida dos usuários antes do acesso. Por meio do programa de parceria RSA Secured, a RSA oferece integração imediata do RSA SecurID com uma série de componentes de infra-estrutura, permitindo que os clientes protejam solidamente o acesso a diferentes sistemas de dados de titulares de cartão.</p>
Requisito 8.5.16: autenticar todo o acesso a qualquer banco de dados que contenha dados de titulares de cartão. Isso inclui acesso por aplicativos, administradores e todos os outros usuários.	<p>A tecnologia RSA SecurID ajuda os clientes a exceder esse requisito, oferecendo métodos de autenticação sólida para os usuários, aplicados antes do acesso aos sistemas de dados de titulares de cartão, além da integração imediata por meio do programa RSA Secured.</p>



©2007 RSA Security Inc. Todos os direitos reservados.

RSA, RSA Security, enVision, SecurID e o logotipo da RSA são marcas comerciais registradas ou marcas comerciais da RSA Security Inc. nos Estados Unidos e/ou em outros países. EMC é marca registrada da EMC Corporation. Todos os outros produtos e serviços mencionados são marcas comerciais de suas respectivas empresas.

PCI SEA SB 0307



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

A Divisão de Segurança da EMC