

Resumo da solução RSA

Gerenciamento de informações de conformidade e segurança para o Requisito 10 do PCI DSS e superior

RSA®

The Security Division of EMC

O DSS (Data Security Standard, padrão de segurança de dados) do PCI (Payment Card Industry, setor de cartões de crédito e débito) impõe uma ampla variedade de requisitos de emissão de relatórios, o que é de vital importância durante a auditoria anual de PCI DSS. Além disso, por meio do Requisito 10, o PCI DSS exige, especificamente, que os comerciantes, bancos e processadores de pagamentos “controlem e monitorem todos os acessos aos recursos de rede e aos dados de titulares de cartão”.

Como os negócios recuam e reconhecem as implicações da emissão de relatórios e do monitoramento do PCI DSS, são feitos os seguintes questionamentos: “Embora a conformidade seja essencial, como a minha organização pode se tornar mais proativa do que reativa e como podemos garantir que o tempo e os investimentos em recursos irão além de nossa iniciativa em PCI DSS?”

Indo além da conformidade com a tecnologia RSA enVision®

As violações de política e segurança ocorrem sem aviso. Independentemente de serem erros inocentes ou tentativas ilegais de acesso a informações particulares, você precisa de visibilidade imediata desses comportamentos para reagir. Essa visibilidade e capacidade de resposta são essenciais para atender à conformidade PCI DSS e, sob uma perspectiva mais ampla, é necessário garantir que todas as informações particulares de clientes, parceiros e negócios de sua organização estejam seguras.

O RSA enVision transforma eventos de segurança e de rede brutos e aparentemente não relacionados em inteligência de negócios significativa. Ao estabelecer primeiro níveis de linha de base de atividade para todo o ambiente de rede, o RSA enVision ajuda a determinar comportamentos fora do padrão e alertas de problemas quando tais atividades ocorrem. Ao capturar todos os dados – desde aplicativos

Vantagens para o cliente: solução de gerenciamento de informações de segurança e conformidade

Com a tecnologia RSA enVision, você terá a oportunidade de:

- Ter a garantia de que se ocorrer a violação de uma política ou segurança, você saberá e poderá reagir.
- Focalizar novamente no crescimento dos negócios – em vez de responder às auditorias –, uma vez que sua organização tem uma ferramenta para ajudar a provar que os principais requisitos do PCI DSS foram atendidos.
- Ir além da conformidade ao aproveitar os investimentos baseados em PCI DSS para melhorar a postura geral de segurança da empresa.

corporativos, de segurança e de rede até dispositivos de mainframe, desktop e de armazenamento – o RSA enVision garante que você tenha visibilidade completa e não-filtrada.

Além da conformidade com o PCI, o RSA enVision elimina os silos de dados de negócios criados em muitas organizações. Ele coleta, analisa e gerencia todos os dados e fornece uma plataforma que ajuda a informar virtualmente qualquer pessoa na organização. Não apenas os auditores de conformidade têm um conjunto completo de dados para resolver os problemas de conformidade, mas as operações de gerenciamento de riscos e de segurança podem visualizar os alertas de segurança em tempo real. Qualquer pessoa, das operações de desktop, ao help desk, até o pessoal de gerenciamento de rede e de aplicativos, pode acessar os relatórios de que precisam a qualquer momento.

Componentes da solução RSA PCI

- > **RSA® Access Manager.** As soluções RSA para acesso corporativo seguro permitem 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 para proteção de dados corporativos.** As soluções RSA de dados corporativos seguros permitem que os negócios afetados pelo padrão PCI protejam os dados dos titulares de cartões em todos os pontos finais de criptografia e gerenciem centralmente 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 de segurança permite que os clientes facilitem os processos de auditoria ao estabelecer um ponto central para controlar e monitorar o acesso aos dados de titulares de cartões em um ambiente do PCI.
- > **RSA SecurID®.** As soluções da RSA para segurança de acesso aos dados corporativos ajudam os clientes a garantir que os usuários que acessam os sistemas de dados de titulares de cartões e a rede de TI mais ampla sejam quem afirmam ser.
- > **RSA Professional Services.** Os RSA Professional Services oferecem diversos recursos, como a ajuda aos clientes para se prepararem para auditorias do PCI DSS, o suporte à ampla detecção de dados de titulares de cartões pela empresa, e a implementação de tecnologias para correções.
- > **EMC Celerra e EMC Centera.** A integração imediata do EMC Celerra e EMC Centera com a tecnologia RSA enVision permite que os clientes armazenem dados essenciais de log de auditoria de PCI de modo econômico.

O RSA enVision aproveita o LogSmart IPDB (Internet Protocol Database, banco de dados de protocolos da Internet) para coletar e analisar as informações de conformidade e segurança da empresa. O LogSmart IPDB mantém uma corrente digital de custódia para todos os dados, uma vez que os dados forem confirmados no banco de dados, eles não poderão ser alterados – diferentemente dos esquemas de dados usados em RDBMS (Relational Database Management System, sistema de gerenciamento de banco de dados relacionais) baseado em soluções.

Além disso, enquanto outras soluções reduzem ou filtram previamente os dados provenientes de dispositivos de origem porque o RDBMS simplesmente não pode mantê-los, o RSA enVision captura os dados completos definidos no LogSmart IPDB. A organização será beneficiada com análises em tempo real e autenticação paralela e com a compactação de dados,

o que significa que os alertas são altamente precisos e oportunos. Os benefícios da coleta sem agentes são claros – sem filtragem de dados na origem, sem gerenciamento contínuo de agentes por toda a rede, sem riscos ou impactos na infra-estrutura de rede e custo total de propriedade menor devido à configuração e implantação fáceis.

Ao final, a tecnologia RSA enVision posiciona os negócios para responder rapidamente às políticas e falhas de segurança, o que ajuda a melhorar a situação de segurança de TI da empresa e facilitar o processo de conformidade. O RSA enVision ajuda a posicionar os clientes para que concentrem os recursos financeiros e humanos em iniciativas de crescimento de negócios, em vez de reagir ao ciclo contínuo de auditorias de PCI DSS.

Para obter mais informações sobre as soluções da RSA para ajudar os clientes a atender à conformidade PCI DSS, visite <http://brazil.rsa.com/>

Requisito 10 de PCI DSS e RSA enVision

REQUISITO DO PCI DSS	RECURSO RSA enVISION
<p>> Requisito 10.1 Estabelecer um processo para vincular todos os acessos aos componentes do sistema (especialmente o acesso feito com privilégios administrativos como o acesso à raiz) para cada usuário individual.</p>	<p>O RSA enVision permite que os clientes controlem as atividades do usuário administrativo e fornece supervisão a fim de ajudar a verificar se um usuário está agindo de acordo com a política estabelecida. Além disso, o sistema pode enviar um alerta ao supervisor do usuário caso o comportamento deste viole a política.</p> <p>O RSA enVision oferece relatórios prontos para uso que exibem todos os escalonamentos de privilégio administrativos que obtiveram êxito em sistemas UNIX e Linux monitorados.</p> <p>Relatório: “PCI – escalonamento de privilégios administrativos – Unix e Linux”</p>
<p>> Requisito 10.2 Implementar trilhas de auditoria automatizadas para todos os componentes do sistema para reconstruir os eventos indicados a seguir</p>	<p>O dispositivo RSA enVision ajuda as empresas a implementar trilhas de auditoria automatizadas que detalham o acesso de usuários aos dados de portadores de cartões, as ações tomadas pelos usuários com privilégios de administrador/root, o acesso a trilhas de auditoria, as tentativas inválidas de acesso lógico, o uso de mecanismos de identificação/autenticação, a inicialização de logs de auditoria e a criação/exclusão de objetos de nível de sistema.</p>
<p>Requisito 10.2.1 Todos os acessos individuais de usuário aos dados de titular do cartão</p>	<p>O RSA enVision oferece recursos de emissão de relatórios do RSA que exibem todas as tentativas de acesso a arquivos que obtiveram êxito no grupo de dispositivos “Titulares de cartões”. Esse grupo de dispositivos é um subconjunto do grupo de dispositivos PCI e deve conter somente os servidores usados no armazenamento de dados dos titulares de cartões.</p> <p>Relatório: “PCI: acessos individuais de usuário aos dados de titular do cartão – Windows”</p>
<p>Requisito 10.2.2 Todas as ações de pessoas com privilégios de administrador ou root</p>	<p>O RSA enVision permite que os clientes emitam relatórios de todas as ações tomadas pelos usuários registrados como “root”. Além disso, as organizações podem personalizar esses relatórios para incluir quaisquer nomes de usuários adicionais que receberam privilégios administrativos de monitoramento de usuários no ambiente.</p> <p>Relatório: “PCI – todas as ações de pessoas com privilégios de administrador ou root – Unix e Linux”</p> <p>A emissão de relatórios do RSA enVision permite que os clientes monitorem todas as ações tomadas pelos usuários registrados como “administrador”. Os clientes podem reforçar ainda mais a proteção ao incluir quaisquer nomes de usuários adicionais que receberam privilégios administrativos no ambiente.</p> <p>Relatório: “PCI – todas as ações de pessoas com privilégios de administrador ou root – Windows”</p>
<p>Requisito 10.2.3 Acesso a todas as trilhas de auditoria</p>	<p>O RSA enVision oferece relatórios incorporados que permitem que os clientes facilmente monitorem todos os logons efetuados com êxito no RSA enVision.</p> <p>Relatório: “PCI – acesso a todas as trilhas de auditoria”</p>
<p>Requisito 10.2.4 Tentativas inválidas de acesso lógico</p>	<p>O RSA enVision permite que os clientes facilmente emitam relatórios das tentativas de acesso que foram negadas devido às restrições da lista de controle de acesso.</p> <p>Relatório: “PCI – tentativas inválidas de acesso lógico – resumo de ACL negada”</p>
<p>Requisito 10.2.5 Uso de mecanismos de identificação e autenticação</p>	<p>O RSA enVision pode permitir que as organizações visualizem facilmente um relatório que detalha todos os acessos dos usuários ao grupo de dispositivos PCI que são autenticados usando os servidores RSA Authentication Manager.</p> <p>Relatório: “PCI – uso de sistemas de identificação e autenticação – RSA”</p>
<p>Requisito 10.2.6 Inicialização de logs de auditoria</p>	<p>O RSA enVision fornece relatórios prontos para uso que oferecem uma visualização da inicialização de logs de auditoria em sistemas operacionais Windows, UNIX, Linux, AIX e HPUX.</p> <p>Relatório: “PCI – inicialização de logs de auditoria”</p>
<p>Requisito 10.2.7 Criação e exclusão de objetos de nível do sistema</p>	<p>Os recursos de emissão de relatório do RSA enVision permitem que os clientes visualizem as exclusões de todos os objetos de nível de sistema em sistemas Windows monitorados, realizadas no grupo de dispositivos “PCI”.</p> <p>Relatório: “PCI – exclusão de objetos de nível de sistema – Windows”</p>

Requisito 10 de PCI DSS e RSA enVision – *continuação*

REQUISITO DO PCI DSS	RECURSO RSA ENVISION
<p>> Requisito 10.3 Registrar pelo menos as seguintes entradas de trilha de auditoria para todos os componentes do sistema em cada evento</p>	<p>O RSA enVision registrará os eventos à medida que forem relatados pelos dispositivos associados. Além disso, o RSA enVision salva os metadados de evento, que podem ser analisados e revisados para determinar o tipo de evento.</p>
<p>Requisito 10.3.1 Identificação de usuário</p>	<p>O RSA enVision permite que as organizações gravem informações de identificação de usuário para cada evento associado ao grupo de dispositivos PCI.</p>
<p>Requisito 10.3.2 Tipo de evento</p>	<p>O RSA enVision permite que as organizações identifiquem informações de tipo de evento para cada evento associado ao grupo de dispositivos PCI. Se o dispositivo não emitir nenhum relatório de tipo de evento, o RSA enVision emitirá relatórios salvando os metadados que podem ser analisados e revisados para determinar o tipo de evento.</p>
<p>Requisito 10.3.3 Data e hora</p>	<p>O RSA enVision permite que as organizações gravem informações de data e hora para cada evento associado ao grupo de dispositivos PCI.</p>
<p>Requisito 10.3.4 Indicação de sucesso ou falha</p>	<p>O RSA enVision permite que as organizações gravem informações com indicação de sucesso/falha para cada evento associado ao grupo de dispositivos PCI.</p>
<p>Requisito 10.3.5 Origem do evento</p>	<p>O RSA enVision permite que as organizações gravem informações de origem de eventos para cada evento associado ao grupo de dispositivos PCI.</p>
<p>Requisito 10.3.6 Identidade ou nome dos dados do componente do sistema ou do recurso afetado</p>	<p>O RSA enVision permite que as organizações gravem o nome ou outra identidade dos sistemas, dados, componentes ou outros recursos do PCI afetados.</p>
<p>> Requisito 10.5 Proteger as trilhas de auditoria de modo que não possam ser alteradas</p>	<p>O RSA enVision fornece dados não-filtrados e espelhados para o banco de dados de protocolos da Internet, o que capacita a retenção do formato original dos dados. Também, os recursos de WORM (Write Once Read Many, uma gravação e várias leituras) ajudam a garantir que as cópias espelhadas permaneçam intactas, mesmo se os dados originais estiverem comprometidos. Os registros de eventos capturados pelo RSA enVision são armazenados em um sistema operacional avançado, compactados e protegidos via criptografia leve.</p>
<p>Requisito 10.5.1 Visualização limitada das trilhas de auditoria para necessidades relacionadas a trabalho</p>	<p>O RSA enVision permite que as organizações atribuam privilégios para que somente os usuários autorizados tenham acesso e visualizem a trilha de auditoria.</p>
<p>Requisito 10.5.2 Proteger os arquivos de auditoria de modificações não-autorizadas</p>	<p>Os registros do RSA enVision não podem ser alterados por meio da GUI (Graphical User Interface, interface gráfica de usuário); as alterações somente podem ocorrer via acesso administrativo ao aplicativo RSA enVision em si. Além disso, o acesso aos dados do RSA enVision e as APIs do arquivamento são somente leitura, portanto, os registros não podem ser alterados no sistema.</p>
<p>Requisito 10.5.3 Realizar imediatamente o backup em arquivos de trilha de auditoria para servidor centralizado de registro ou mídia que seja difícil de alterar</p>	<p>O RSA enVision permite que os backups de trilhas de auditoria sejam programados com a frequência necessária para o servidor centralizado de registro ou outra mídia – por exemplo, a cada 10 minutos ou a cada hora, dependendo da necessidade do cliente.</p> <p>O RSA enVision oferece uma API (Application Program Interface, interface de programas aplicativos) de “manutenção LS” que permite que os usuários programem backups em um dispositivo ou grupo de dispositivos (por exemplo, grupo de dispositivos PCI). Os clientes teriam a capacidade de, por exemplo, programar backups do PCI a cada 10 minutos, ao mesmo tempo que poderiam ser feitos backups diários dos dispositivos fora do escopo do PCI.</p>

Requisito 10 de PCI DSS e RSA enVision — *continuação*

REQUISITO DO PCI DSS	RECURSO RSA enVISION
<p>Requisito 10.5.5 Usar monitoramento de integridade de arquivos e software de detecção de alterações em registros para garantir que os dados de registro atuais não sejam alterados sem a geração de alertas (embora os dados novos adicionados não causem um alerta)</p>	<p>O RSA enVision é capaz de criar alertas que garantem que os supervisores e outras pessoas tomem conhecimento de qualquer alteração efetuada nos registros. Além disso, a tecnologia RSA enVision com base em aplicativos é baseada em sistema operacional avançado que fornece graus mais altos de segurança.</p>
<p>> Requisito 10.7 Manter o histórico de trilha de auditoria por pelo menos um ano, com um mínimo de três meses de disponibilidade on-line</p>	<p>O RSA enVision NAS3500 oferece o EMC Celerra pré-configurado, pré-testado e em rack, permitindo que os clientes tenham entre 3,5 TB e 7 TB de armazenamento – número especialmente relevante para a retenção de dados de registro on-line.</p> <p>Além disso, como o RSA enVision é projetado para ter integração imediata com as plataformas de armazenamento em rede como EMC® Centera™ e EMC Celerra®, os clientes são capazes de armazenar as informações essenciais para atender aos requisitos de conformidade.</p> <p>Os sistemas do EMC Celerra NAS (Network Attached Storage, armazenamento conectado à rede) fornecem o preço/desempenho líder do setor com disponibilidade sem comprometimento. A disponibilidade sem comprometimento significa que os aplicativos continuam executando as operações nos mesmos níveis de desempenho e serviço, mesmo em caso de falha. O Celerra consegue fazer isso por meio de uma arquitetura de cluster N+1 ativa-passiva e eliminando qualquer ponto de falha da rede até o drive de disco.</p> <p>Os sistemas do EMC Celerra NAS implementam um recurso chamado “File Level Retention”, que fornece proteção WORM baseada em disco para arquivos. Esse recurso do Celerra protege arquivos e diretórios de serem excluídos, alterados, renomeados ou substituídos durante o período de retenção especificado. O Celerra File Level Retention pode oferecer às organizações a capacidade de proteger a integridade de logs de auditoria por um período de retenção específico (por exemplo, três meses).</p>

Requisito 10 de PCI DSS e RSA enVision

O Requisito 10 de PCI DSS afirma que as empresas devem “controlar e monitorar todo o acesso aos recursos de rede e aos dados do titular do cartão”. O RSA enVision permite que os clientes facilitem os processos de auditoria ao estabelecer um ponto central para controlar e monitorar o acesso aos dados de titulares de cartões ao longo de um ambiente do PCI. Alguns recursos específicos que o RSA enVision oferece para atender ao padrão PCI DSS são:

Além de sua capacidade principal em ajudar os clientes a atender ao Requisito 10 de PCI DSS, a tecnologia RSA enVision oferece uma plataforma robusta para o acesso à coleta, correlação e auditoria em uma ampla gama de sistemas de PCI – desde firewalls até redes sem fio para mecanismos de autenticação e mais. A tecnologia ajuda os clientes a atender aos principais requisitos do PCI DSS ao:

- Fornecer um conjunto robusto de relatórios de atividade

do firewall para validar rapidamente a conformidade com o Requisito 1 (“Instalar e manter uma configuração de firewall para proteger os dados de titulares de cartão”).

- Permitir que os clientes atendam aos locais das chaves do Requisito 2 (“Não usar os padrões dos fornecedores para a senha do sistema e outros parâmetros de segurança”), ao emitir relatórios com facilidade sobre as alterações de configuração feitas em ambientes sem fio.
- Ajudar a facilitar o processo de emissão de relatórios sobre atualizações para sistemas antivírus corporativos para respaldar o Requisito 5 (“Usar e atualizar regularmente um software antivírus”).
- Apoiar trabalhos para provar a conformidade com o Requisito 6 (“Desenvolver e manter sistemas e aplicativos seguros”), ao emitir relatórios sobre patches e aplicativos de serviço.

Emissão de relatórios e auditoria PCI DSS e RSA enVision

REQUISITO DO PCI DSS

RECURSO RSA enVISION

> Requisito 1.1

Estabelecer os padrões de configuração de firewall que incluem:

<p>Requisito 1.1.1 Um processo formal para a aprovação e testes de todas as conexões de rede externas e alterações da configuração de firewall</p>	<p>O RSA enVision oferece suporte à conformidade ao fornecer relatórios prontos para uso que exibem todas as alterações de configuração de firewalls do grupo de dispositivos PCI.</p> <p>Relatório: “PCI – alterações de configuração em firewalls”</p>
<p>Requisito 1.1.5 Lista documentada de serviços e portas necessárias para os negócios</p>	<p>O RSA enVision fornece emissão de relatórios incorporada para resumir todo o tráfego de firewall por porta no grupo de dispositivos PCI.</p> <p>Relatório: “PCI – tráfego por porta – grupo de dispositivos PCI”</p>
<p>Requisito 1.1.6 Justificativas e documentação para qualquer protocolo disponível além do HTTP (Hypertext Transfer Protocol, protocolo de transferência de hipertexto), SSL (Secure Sockets Layer, camada de soquetes segura), SSH (Secure Shell) e VPN (Virtual Private Network, rede virtual privada)</p>	<p>O RSA enVision fornece modelos de relatórios prontos para serem executados que detalham todo o tráfego de firewall por porta para endereços IP (Internet Protocol, protocolo de Internet) especificados como um parâmetro de tempo de execução, no qual a porta usada não está justificada diretamente por PCI.</p> <p>Relatório: “PCI – tráfego para portas não-padrão – detalhes”</p> <p>Os relatórios do RSA enVision resumem todo o tráfego de firewall por porta do computador de destino, no qual a porta usada não é justificada diretamente pelo PCI.</p> <p>Relatório: “PCI – tráfego para portas não-padrão – resumo”</p>
<p>Requisito 1.1.8 Revisão trimestral dos conjuntos de regras do firewall e do roteador</p>	<p>A emissão de relatórios do RSA enVision facilita a conformidade ao fornecer relatórios prontos para uso que exibem todas as alterações de configuração feitas nos firewalls do grupo de dispositivos PCI.</p> <p>Relatório: “PCI – alterações de configuração em firewalls”</p>
<p>Requisito 1.1.9 Padrões de configuração para roteadores</p>	<p>Os modelos do RSA enVision permitem que os clientes facilmente exibam todas as alterações de configuração feitas nos roteadores do grupo de dispositivos PCI.</p> <p>Relatório: “PCI – alterações de configuração em roteadores”</p>

Emissão de relatórios e auditoria PCI DSS e RSA enVision – *continuação*

REQUISITO DO PCI DSS	RECURSO RSA ENVISION
<p>> Requisito 1.3 Criar uma configuração de firewall que restrinja as conexões entre servidores de acesso público e qualquer componente do sistema que armazene dados de titulares de cartão, inclusive qualquer conexão de redes sem fio. Esta configuração de firewall deve abranger:</p>	
<p>Requisito 1.3.1 Restringir o tráfego de entrada de Internet para endereços IP na DMZ (filtros de ingresso)</p>	<p>Os recursos de emissão de relatórios do RSA enVision permitem que os clientes automaticamente listem todo o tráfego de entrada de Internet em portas não-padrão no grupo de dispositivos PCI de forma detalhada e resumida. Relatório: “PCI – tráfego de saída de Internet em portas não-padrão – detalhes”</p>
<p>Requisito 1.3.2 Não permitir que os endereços internos passem da Internet para uma DMZ (DeMilitarized Zone, zona desmilitarizada)</p>	<p>O RSA enVision fornece modelos incorporados que permitem que os clientes facilmente emitam relatórios sobre todo o tráfego de entrada de Internet em portas não-padrão no grupo de dispositivos PCI de forma detalhada e resumida. Relatório: “PCI – tráfego de saída de Internet em portas não-padrão – detalhes”</p>
<p>Requisito 1.3.6 Proteção e sincronização de arquivos de configuração de roteadores. Por exemplo, a execução de arquivos de configuração (para o funcionamento normal de roteadores) e a inicialização de arquivos de configuração (quando as máquinas forem reinicializadas) devem ter a mesma configuração protegida</p>	<p>O RSA enVision oferece relatórios incorporados que resumem todo o tráfego de saída por destino. Relatório: “PCI – resumo do tráfego de saída” O RSA enVision relata detalhes de todo o tráfego de saída para um endereço IP. Relatório: “PCI – detalhes do tráfego de saída por endereço de origem”</p>
<p>Requisito 2.1.1 Em ambientes sem fio, alterar os padrões do fornecedor, incluindo, mas não se limitando a, chaves com WEP, SSID, senhas e caracteres da comunidade SNMP. Desativar transmissões de SSID. Ativar a tecnologia de acesso WiFi protegido (WPA e WPA2) para criptografia e autenticação quando compatível com WAP.</p>	<p>O RSA enVision oferece relatórios predefinidos que detalham todas as alterações de configuração feitas em roteadores sem fio, permitindo que os clientes facilmente demonstrem para um auditor que os padrões do fornecedor – como chaves WEP (Wired Equivalent Privacy, privacidade equivalente com fio), SSID (Default Service Set Identifier, identificador de conjuntos padrão de serviço) padrão, caracteres da comunidade SNMP (Simple Network Management Protocol, protocolo simples de gerenciamento de rede) e desabilitação de transmissões de SSID – foram alterados antes que o roteador sem fio fosse introduzido ao ambiente de cartões de crédito e débito. Relatório: “PCI – alterações de configuração em ambientes sem fio”</p>
<p>> Requisito 3.6 Documentar e implementar completamente todos os processos e procedimentos de gerenciamento de chaves para as chaves usadas na criptografia dos dados de titulares de cartão.</p>	<p>O RSA enVision fornece relatórios predefinidos que permitem que os clientes detalhem toda a geração e a alteração de períodos das chaves de criptografia usadas no armazenamento seguro e na transferência de dados de cartões de crédito e débito, além de resumir os detalhes de controle de acesso como logons que falharam e obtiveram êxito, aplicação de políticas e emissão de relatórios regulares.</p>
<p>> Requisito 4.1 Usar protocolos sólidos de criptografia e segurança, como SSL/TLS (Transport Layer Security, segurança de camada de transporte) e IPSEC (Internet Protocol Security, segurança do protocolo de Internet) para proteger dados confidenciais de titulares de cartão durante a transmissão por redes abertas e públicas. Exemplos de redes abertas e públicas que estão no escopo do PCI DSS são a Internet, WiFi (IEEE 802.11x), comunicação por GSM (Global System for Mobile, sistema global para telefonia) e GPRS (General Packet Radio Service, pacote de serviços gerais de rádio).</p>	<p>Os recursos de emissão de relatórios do RSA enVision permitem que os clientes acessem todas as operações de criptografia, nas quais o uso da criptografia falhou ou foi desabilitado pelo usuário. Relatório: “PCI – falhas de transmissão criptografadas”</p>

Emissão de relatórios e auditoria PCI DSS e RSA enVision – *continuação*

REQUISITO DO PCI DSS	RECURSO RSA ENVISION
<p>> Requisito 5.2 Assegurar que todos os mecanismos antivírus estejam atualizados, sendo executados ativamente e sejam capazes de gerar registros de auditoria</p>	<p>O RSA enVision oferece modelos de emissão de relatórios que facilitam os procedimentos de atualização de revisões por parte dos administradores e auditores para sistemas antivírus. Relatório: “PCI – procedimentos de atualização de antivírus”</p>
<p>> Requisito 6.1 Assegurar que todos os componentes do sistema e produtos de software tenham instalados os mais recentes patches de segurança fornecidos pelo fabricante. Instalar os patches de segurança relevantes até um mês após o lançamento</p>	<p>O RSA enVision fornece relatórios incorporados que oferecem uma visualização de todos os aplicativos de patches e service packs para sistemas baseados em Microsoft Windows. Relatório: “PCI – aplicativo de patch fornecido pelo fabricante”</p>

A RSA é seu parceiro confiável

A RSA, divisão de segurança da EMC, é especializada em segurança centrada nas informações, permitindo a proteção ao longo de todo o ciclo de vida. A RSA permite aos clientes proteger, a custos reduzidos, suas informações mais importantes e identidades on-line, onde quer que se encontrem e em qualquer situação, além de gerenciar informações e eventos de segurança, reduzindo a carga representada pela conformidade.

A RSA oferece as melhores soluções do setor quanto a segurança de identidade e controle de acesso; gerenciamento de chaves e criptografia; gerenciamento de informações de segurança e conformidade, e proteção contra fraude. Essas soluções geram confiança nas identidades de milhões de usuários, às transações que eles executam e aos dados gerados. Para obter mais informações, visite os sites <http://brazil.rsa.com> e <http://brazil.emc.com>.

©2007 RSA Security Inc. Todos os direitos reservados. RSA, enVision, SecurID e o logo da RSA são marcas 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 seus respectivos proprietários.

PCISIEM SB 0307



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

The Security Division of EMC