



Programa Visanet

Segurança da Informação

**Indústria de Cartões de Pagamento
Padrão de Segurança de Dados**

Versão 1.1 -08/2005

Documento PVSI-005/05

O Documento Programa Visanet de Segurança da Informação – Indústria de cartões de pagamento, padrões de segurança de dados, define práticas que são aceitáveis pela Visanet e Visa Internacional para a proteção das informações de cartões e das transações. Apesar de todo o cuidado em sua elaboração, a Visanet e a Visa, não garantem que a implementação desses padrões irá evitar completamente a incidência de qualquer falha de segurança ou perda de informações e se isentam de qualquer responsabilidade ou sanções legais por quaisquer falhas de segurança ou perdas ocorridas, mesmo se os padrões aqui definidos tenham sido implementados em sua íntegra ou parcialmente.



Indústria de Cartões de Pagamento Padrão de Segurança de Dados

Construa e Mantenha Uma Rede Segura

- Exigência 1: Instale e mantenha uma configuração de firewall para proteger os dados
- Exigência 2: Não use as senhas padrões de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços

Proteja os Dados do Portador de Cartão

- Exigência 3: Proteja os dados armazenados
- Exigência 4: Codifique a transmissão dos dados do portador de cartão e as informações importantes que transitam nas redes públicas

Mantenha um Programa de Administração da Vulnerabilidade

- Exigência 5: Use e atualize regularmente o software antivírus
- Exigência 6: Desenvolva e mantenha seguros os sistemas e aplicativos

Implemente Medidas Rígidas de Controle ao Acesso

- Exigência 7: Restrinja o acesso aos dados a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos
- Exigência 8: Atribua um ID único para cada pessoa que possua acesso ao computador
- Exigência 9: Restrinja ao máximo o acesso físico aos dados do portador de cartão

Acompanhe e Teste Regularmente as Redes

- Exigência 10: Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão
- Exigência 11: Teste regularmente os sistemas e os processos de segurança

Mantenha uma Política de Segurança da Informação

- Exigência 12: Mantenha uma política que atenda à segurança da informação

Note que estas Exigências de Segurança de Dados da Indústria de Cartão de Pagamento (PCI) se aplicam a todos os Membros, estabelecimentos e prestadores de serviços que armazenem, processem ou transmitam os dados dos portadores de cartões. Adicionalmente, estas exigências de segurança se aplicam a todos os "componentes do sistema" os quais são definidos como qualquer componente de rede, servidor ou aplicativo incluído, ou conectado ao ambiente de dados do portador de cartão. Os componentes de rede incluem, mas não estão limitados a, firewalls, switches, routers, pontos de acesso

wireless, dispositivos de rede e outros dispositivos de segurança. Os servidores incluem, mas não estão limitados a, web, banco de dados, autenticação, DNS, mail, proxy, e NTP. Aplicativos incluem todos os aplicativos adquiridos e personalizados, incluindo os aplicativos (web) internos e externos.

Construa e Mantenha uma Rede Segura

Exigência 1: Instale e mantenha uma configuração de firewall para proteger os dados.

Os firewalls são dispositivos que controlam o tráfego externo via computador admitido na rede da empresa, bem como o tráfego em áreas mais críticas dentro da rede interna da empresa. Todos os sistemas devem ser protegidos contra o acesso não autorizado através da Internet, seja ele via e-commerce, acesso dos funcionários com base na Internet e via desktop browsers, ou acesso via e-mail de funcionários. Geralmente, os caminhos aparentemente insignificantes para entrar e sair da Internet podem propiciar um acesso desprotegido a sistemas importantes. O firewall é o principal mecanismo de proteção de qualquer rede de computador.

1.1 Estabeleça um padrão de configuração de firewall que inclua:

- 1.1.1** Um processo formal de aprovação e teste de todas as conexões externas e mudanças na configuração do firewall
- 1.1.2** Um diagrama atualizado da rede com todas as conexões que levem aos dados do portador de cartão, incluindo qualquer rede wireless
- 1.1.3** Exigências para um firewall em cada conexão com a Internet e entre qualquer DMZ e a Intranet
- 1.1.4** Descrição dos grupos, tarefas e responsabilidades para a administração lógica dos componentes da rede
- 1.1.5** Lista documentada dos serviços/ports necessários para o negócio
- 1.1.6** Justificação e documentação de qualquer outro protocolo disponível além do http, SSL, SSH, e VPN
- 1.1.7** Justificativa e documentação de qualquer protocolo de risco permitido (FTP, etc.), que inclua a razão para o uso do protocolo e características de segurança implementadas
- 1.1.8** Revisão periódica dos conjuntos de regras para o firewall/router
- 1.1.9** Padrão de configuração para os routers

1.2 Construa uma configuração de firewall que não permita qualquer tráfego advindo das redes/hosts, não confiáveis, **com exceção de:**

- 1.2.1** Protocolos da web - HTTP (port 80) e Secure Sockets Layer (SSL) (geralmente port 443)
- 1.2.2** Protocolos de administração de sistema (ex: Secure Shell (SSH) ou Virtual Private Network (VPN))
- 1.2.3** Outros protocolos requeridos pelo negócio (ex: para o ISO 8583).

1.3 Construa uma configuração de firewall que restrinja as conexões entre os servidores de acesso público e qualquer componente do sistema que armazene os dados do portador de cartão, incluindo quaisquer conexões de redes wireless. Esta configuração de firewall deve incluir:

- 1.3.1** Restrição ao tráfego de entrada da Internet aos endereços de IP dentro da DMZ (filtros de ingresso)
- 1.3.2** Restrição do tráfego da Internet de entrada e saída nos ports 80 e 443

- 1.3.3 Não permita que os endereços internos passem da Internet para a DMZ (filtros de ingresso)
 - 1.3.4 Inspeção *stateful*, também conhecida como dynamic packet filtering (são apenas permitidas as conexões "instaladas" nesta rede)
 - 1.3.5 Colocação do banco de dados em uma zona interna da rede, separada da DMZ
 - 1.3.6 Restrição do tráfego de saída apenas para o que for necessário ao ambiente de cartões de pagamento
 - 1.3.7 Arquivos de configuração de router seguros e sincronizados (ex: arquivos de configuração de execução – usados para o funcionamento normal dos routers e arquivos de configuração de partida – usados quando as máquinas são religadas, devem possuir a mesma configuração segura)
 - 1.3.8 Bloqueio de qualquer outro tráfego de entrada e saída que não seja especificamente permitido
 - 1.3.9 Instalação de um perímetro de firewalls entre quaisquer redes wireless e as redes e o ambiente de cartões de pagamento e configuração destes firewalls para bloquear ou controlar (se tal tráfego for necessário para o objetivo do negócio) qualquer tráfego do ambiente wireless
 - 1.3.10 Instalação de um software de firewall individual em qualquer dispositivo portátil e/ou computador de propriedade do funcionário que possua conexão direta com a Internet (ex: laptops usados pelos funcionários), os quais sejam usados para o acesso à rede da organização
- 1.4 Proíba o acesso público direto entre as redes externas e qualquer componente do sistema de armazenagem da informação do portador de cartão (ex: banco de dados)
- 1.4.1 Implementação de uma DMZ para filtrar e verificar todo o tráfego e para bloquear qualquer rota direta para a entrada e saída do tráfego da Internet
 - 1.4.2 Restrição do tráfego de saída dos aplicativos de cartões de pagamento para os endereços de IP dentro da DMZ.
- 1.5 Implemente o Internet Protocol (IP) disfarçado de forma a impedir que os endereços internos sejam traduzidos e revelados na Internet. Use tecnologias que implementem o espaço de endereço RFC 1918, tais como Port Address Translation (PAT) ou Network Address Translation (NAT)

Exigência 2: Não use as senhas padrões de sistema e parâmetros de segurança fornecidos pelos prestadores de serviços.

Hackers (externos e internos à empresa) geralmente usam as senhas padrão dos prestadores de serviços e outros parâmetros padrões para comprometer os sistemas. Estas senhas e parâmetros são bastante conhecidas nas comunidades de hackers e facilmente obtidas através de informações públicas.

- 2.1 Troque sempre os padrões estabelecidos pelo prestador de serviço **antes** da instalação de um sistema na rede (ex: senhas, SNMP community strings, e eliminação de contas desnecessárias).
- 2.1.1 Nos ambientes wireless, mudar os padrões de wireless do prestador de serviço, incluindo mas não limitado a, chaves WEP, padrão SSID, senhas, e SNMP community strings e desativação da transmissão de SSID. Ativar a tecnologia de Wi-Fi Protected Access (WPA) para a codificação e autenticação quando for capacitado a operar a WPA.

- 2.2** Desenvolva uma configuração padrão para todos os componentes do sistema. Certifique-se de que estes padrões atendam a todas as vulnerabilidades conhecidas e às melhores práticas da indústria.
- 2.2.1** Implemente apenas uma função principal por servidor (ex: *servidores da web, servidores de banco de dados e DNS devem ser implementados em servidores separados*)
 - 2.2.2** Desative todos os serviços e protocolos inseguros e desnecessários (*serviços e protocolos não diretamente necessários para executar a função específica do dispositivo*)
 - 2.2.3** Configure os parâmetros de segurança do sistema para prevenir o uso incorreto
 - 2.2.4** Remova todas as funcionalidades desnecessárias, tais como scripts, drivers, características, sub-sistemas, sistemas de arquivo (ex: servidores de web desnecessários).
- 2.3** Codifique todo o acesso administrativo que não seja via teclado. Use tecnologias tais como SSH, VPN, ou SSL/TLS para a administração baseada na web e outro acesso administrativo via unidade de teclado.

Proteja os Dados do Portador de Cartão

Exigência 3: Proteja os Dados Armazenados

A codificação é o mecanismo que oferece a máxima proteção porque mesmo que alguém consiga ter acesso ao dado codificado, este não será capaz de ler o dado sem antes descobrir a chave do código. Isto é uma demonstração do princípio de defesa total.

- 3.1** Mantenha em um tamanho mínimo a informação armazenada do portador de cartão. Desenvolva uma política de retenção e destruição de dados. Limite o tempo e a quantidade de dados retidos exclusivamente para o que é necessário ao negócio e com propósitos legais e/ou regulamentares, conforme documentado no regulamento de retenção de dados.
- 3.2** Não armazene dados críticos de autenticação após a autorização (nem mesmo codificados):
 - 3.2.1** Não armazene o conteúdo total de qualquer trilha da tarja magnética (no verso de um cartão, em um chip, etc.)
 - 3.2.2** Não armazene o código de validação do cartão (valor de três ou quatro dígitos impressos na frente ou verso de um cartão de pagamento (ex: dados do CVV2 e CVC2))
 - 3.2.3** Não armazene o Valor de Verificação do PIN (PIN Verification Value - PVV)
 - 3.3** Oculte os números das contas quando exibidos (os primeiros seis ou quatro últimos dígitos são o maior número de dígitos que devem ser mostrados). *Note que isto não se aplica àqueles funcionários e outros que possuam a necessidade específica de ver o número completo do cartão de crédito.*
 - 3.4** Torne ilegíveis as informações confidenciais dos dados do portador de cartão em qualquer local em que seja armazenado (incluindo os dados em mídia portátil, mídia de backup, em relatórios e dados recebidos ou armazenados por redes wireless) através do uso de qualquer uma das seguintes técnicas:
 - One-way hashes (hashed indexes), tal como SHA-1
 - Truncagem
 - Tokens de indexação e PADs, com os PADs sendo armazenados de forma segura

- Codificação rigorosa, tal como Triple-DES 128-bit ou AES 256-bit associado com processos e procedimentos de administração de chave
 - A informação MÍNIMA da conta que necessita ser tornada ilegível é o número da conta do cartão de pagamento.*
- 3.5** Proteja as chaves de codificação contra a divulgação e o uso indevido.
 - 3.5.1** Restrinja o acesso às chaves ao menor número de custódios necessários
 - 3.5.2** Guarde as chaves de forma segura no menor número de modalidades e lugares
- 3.6** Documente completamente e implemente a totalidade dos processos e procedimentos de administração das chaves, incluindo:
 - 3.6.1** Geração de chaves fortes
 - 3.6.2** Distribuição de chaves seguras
 - 3.6.3** Armazenamento seguro das chaves
 - 3.6.4** Mudança periódica das chaves
 - 3.6.5** Destruição das chaves antigas
 - 3.6.6** Conhecimento compartilhado e duplo controle das chaves (sendo necessária a existência de duas ou três pessoas, cada uma conhecendo apenas a sua parte da chave, para reconstruir a chave inteira).
 - 3.6.7** Prevenção contra a substituição não autorizada das chaves
 - 3.6.8** Reposição das chaves conhecidas ou suspeitas de comprometimento
 - 3.6.9** Cancele as chaves antigas ou inválidas (principalmente as chaves RSA)
 - 3.6.10** Exija que os custódios das chaves assinem um documento especificando que eles compreendem e aceitam as responsabilidades de custódios das chaves

Exigência 4: Codifique a transmissão dos dados do portador de cartão e as informações importantes que transitam nas redes públicas.

As informações confidenciais devem ser codificadas durante a transmissão através da Internet, porque é fácil e comum que um hacker intercepte e/ou redirecione o dado quando em trânsito.

- 4.1** Use técnicas de codificação e cifragem rigorosas (pelo menos de 128 bit) tais como as Secure Sockets Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSEC) para proteger os dados confidenciais do portador de cartão durante a transmissão através das redes públicas
 - 4.1.1** Para as redes wireless transmitindo os dados do portador de cartão, codifique as transmissões através do uso da tecnologia Wi-Fi Protected Access (WPA) se aceitar WPA, ou VPN ou SSL com 128-bit. Nunca confie exclusivamente no WEP para proteger a confidencialidade e acesso para uma LAN wireless. Use uma das metodologias acima em conjunto com WEP de 128 bit, faça a rotatividade trimestral das chaves WEP compartilhadas e sempre que houver mudanças de funcionários.
- 4.2** Nunca envie a informação do portador de cartão através de um e-mail não codificado.

Mantenha um Programa de Administração da Vulnerabilidade

Exigência 5: Use e atualize regularmente o software ou programas antivírus.

Muitas das vulnerabilidades e vírus maliciosos entram na rede através das atividades de e-mail dos funcionários. Deve ser usado um software antivírus em todos os sistemas de e-mail e desktops para proteger os sistemas contra estes softwares maliciosos.

- 5.1** Instale mecanismos antivírus em todos os sistemas comumente afetados por vírus (ex: PC's e servidores).
- 5.2** Assegure-se de que todos os mecanismos antivírus estejam atualizados, rodando ativamente e capazes de gerar logs para auditoria.

Exigência 6: Desenvolva e mantenha sistemas e aplicativos seguros

Indivíduos inescrupulosos usam as vulnerabilidades de segurança para obter acesso privilegiado aos sistemas. Muitas destas vulnerabilidades são resolvidas através de patches de segurança do prestador de serviço, e todos os sistemas devem estar com seus patches atualizados para se proteger contra o abuso por parte dos funcionários, hackers externos e vírus. Para os aplicativos desenvolvidos in-house, muitas das inúmeras vulnerabilidades podem ser evitadas através do uso de processos padrão de desenvolvimento de sistemas e técnicas de codificação seguras.

- 6.1** Assegure-se de que todos os componentes do sistema e software possuem instalados os mais recentes patches de segurança fornecidos pelo prestador de serviço.
 - 6.1.1** Instale os patches de segurança em até um mês após o lançamento.
 - 6.2** Estabeleça um processo para identificar as vulnerabilidades de segurança recém descobertas (ex: assinatura de serviços de alerta disponíveis gratuitamente na Internet). Atualize os seus padrões para fazer face às novas modalidades de vulnerabilidade.
- 6.3** Desenvolva software e aplicativos baseados nas melhores práticas da indústria e inclua a segurança da informação ao longo de todo o ciclo de desenvolvimento do programa. Deve ser incluído o seguinte:
 - 6.3.1 Teste de todos os patches de segurança e mudanças das configurações do sistema e software antes da implantação
 - 6.3.2 Ambientes de desenvolvimento, teste e produção separados
 - 6.3.3 Separação dos ambientes e tarefas de desenvolvimento, teste e produção
 - 6.3.4 Não usar os dados de produção reais (números reais dos cartões de crédito) para teste ou desenvolvimento
 - 6.3.5 Remoção dos dados de teste e contas antes que os sistemas de produção se tornem ativos
 - 6.3.6 Remoção das contas personalizadas, nome do usuário e senhas antes que os aplicativos se tornem ativos ou sejam liberados para os clientes.
 - 6.3.7 Revisão dos códigos customizados antes da liberação para a produção ou clientes, para identificação de qualquer vulnerabilidade potencial do código
 - 6.4** Acompanhe as mudanças nos procedimentos de controle de todo o sistema e mudanças na configuração do software. Os procedimentos devem incluir:
 - 6.4.1** Documentação do impacto

- 6.4.2 Administração do “sign-off” para as partes apropriadas
- 6.4.3 Teste que verifique a funcionalidade operacional
- 6.4.4 Procedimentos de back-out.
 - 6.5 Desenvolva software de web e aplicativos baseados em diretrizes de codificação seguras tais como as diretrizes do Open Web Application Security Project. Revise o código dos aplicativos customizados para identificar vulnerabilidades do código. Consulte www.owasp.org - “The Ten Most Critical Web Application Security Vulnerabilities”. Verifique a prevenção das vulnerabilidades mais comuns no processo de desenvolvimento dos códigos dos softwares para incluir:
 - 6.5.1 Input não validado
 - 6.5.2 Quebra do controle de acesso (ex: uso desonesto dos IDs dos usuários)
 - 6.5.3 Quebra da administração de autenticação/sessão (uso das credenciais da conta e cookies da sessão)
 - 6.5.4 Ataques ao cross-site scripting (XSS)
 - 6.5.5 Overflow do buffer
 - 6.5.6 Defeitos de injection (ex: SQL injection)
 - 6.5.7 Administração incorreta dos erros
 - 6.5.8 Armazenagem insegura
 - 6.5.9 Recusa de serviço
 - 6.5.10 Administração de configuração insegura.

Implemente Medidas Rígidas de Controle ao Acesso

Exigência 7: Restrinja o acesso aos dados a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos.

Isto garante que os dados críticos possam apenas ser acessados de forma autorizada.

- 7.1 Limite o acesso aos recursos de computação e informação do portador de cartão a apenas aqueles indivíduos cuja execução de tarefa exija tal acesso.
- 7.2 Estabeleça um mecanismo para os sistemas com múltiplos usuários que restrinja o acesso baseado na necessidade e o ajuste para “negar tudo” a menos que especificamente autorizado.

Exigência 8: Atribua um ID único para cada pessoa que possua acesso ao computador.

Isto assegura que as ações tomadas com respeito aos dados e sistemas críticos sejam executadas por usuários conhecidos e autorizados que possam ser acompanhados e verificados.

- 8.1 Identifique todos os usuários com um nome de usuário único antes que tenham permissão para acessar os componentes do sistema ou os dados do portador de cartão.
- 8.2 Utilize pelo menos um dos métodos abaixo, em adição a uma identificação exclusiva, para autenticar todos os usuários:
 - Senha

- Dispositivos de identificação física (ex: ID de Segurança, certificados ou chaves públicas)
 - Autenticação Biométrica.
- 8.3** Implemente a autenticação por dois fatores para o acesso remoto à rede pelos funcionários, administradores e prestadores de serviço. Use tecnologias tais como RADIUS ou TACACS com tokens ou VPN com certificados individuais.
- 8.4** Codifique todas as senhas durante a transmissão e armazenamento em todos os componentes do sistema.
- 8.5** Garanta a autenticação eficiente do usuário e administração da senha para os usuários não consumidores e administradores em todos os componentes do sistema:
- 8.5.1** Controle a adição, exclusão e modificação dos IDs dos usuários, credenciais e outros métodos de identificação.
- 8.5.2** Verifique a identidade do usuário antes de executar a mudança de senhas.
- 8.5.3** Estabeleça senhas de uso inicial com um valor único por usuário e faça uma mudança imediata após ser usada pela primeira vez.
- 8.5.4** Revogue imediatamente o acesso por usuários cancelados.
- 8.5.5** Remova as contas de usuários inativos pelo menos a cada 90 dias
- 8.5.6** Habilite as contas usadas pelos prestadores de serviço para a manutenção remota apenas durante o tempo estritamente necessário
- 8.5.7** Distribua os procedimentos de senha e os regulamentos para todos os usuários que possuam acesso à informação do portador de cartão
- 8.5.8** Não utilize senhas ou contas genéricas, de grupo ou compartilhadas
- 8.5.9** Mude as senhas dos usuários pelo menos a cada 90 dias
- 8.5.10** Exija uma senha com o comprimento mínimo de pelo menos sete caracteres
- 8.5.11** Use senhas contendo caracteres tanto numéricos como alfabéticos
- 8.5.12** Não permita que um indivíduo submeta uma nova senha que seja idêntica a qualquer uma das quatro últimas que ele usou
- 8.5.13** Limite a tentativa de acesso repetido por razão de bloqueio do ID do usuário a não mais de seis tentativas
- 8.5.14** Ajuste a duração do bloqueio para trinta minutos ou até que o administrador habilite o ID do usuário
- 8.5.15** Se uma sessão estiver inativa por mais de 15 minutos, exija que o usuário entre outra vez a senha para reativar o terminal
- 8.5.16** Autentique todo o acesso para qualquer banco de dados contendo informações do portador de cartão. Estes incluem o acesso via aplicativos, administradores e todos os demais usuários.

Exigência 9: Restrinja ao máximo o acesso físico aos dados do portador de cartão

Qualquer acesso físico aos dados ou sistemas que abrigam os dados do portador de cartão cria uma oportunidade para acessar dispositivos ou dados e remover sistemas ou cópias físicas e portanto devem ser devidamente restritos.

- 9.1** Use os controles adequados para a admissão nas instalações, limite e controle o acesso físico aos sistemas que armazenam, processam ou transmitem os dados do portador de cartão.
- 9.1.1** Use câmaras para monitorar áreas críticas. Faça a auditoria destes dados e faça a correlação com outras entradas. Armazene estes dados por pelo menos três meses, a menos que proibido por lei.
- 9.1.2** Restrinja o acesso físico às tomadas de acesso público à rede.
- 9.1.3** Restrinja o acesso físico aos pontos de acesso para wireless, portais, e dispositivos portáteis.
- 9.2** Desenvolva procedimentos para auxiliar os funcionários a distinguir entre funcionários e visitantes, especialmente nas áreas onde a informação do portador de cartão pode ser acessada.
- “Funcionário” é definido como empregados de meio expediente e tempo integral, temporários, estagiários e consultores que são “residentes” na instalação da empresa. Um “visitante” é definido como um fornecedor, prestador de serviço, convidado de um funcionário, pessoal de manutenção e serviço ou qualquer um que necessite entrar nas instalações por um curto período de tempo, geralmente por não mais do que um dia.*
- 9.3** Certifique-se de que todos os visitantes são:
- 9.3.1** Autorizados antes de entrar nas áreas onde os dados do portador de cartão são processados ou mantidos
- 9.3.2** Recebam uma identificação física (ex: crachá ou dispositivo de acesso) que tenha vencimento e que os identifique como não funcionários
- 9.3.3** Sejam solicitados a retornar a identificação física antes de deixar a instalação ou por ocasião do vencimento.
- 9.4** Use um registro de visitantes para ter uma evidência física das atividades dos visitantes com a finalidade de auditoria. Mantenha este registro por no mínimo três meses, a menos que proibido por lei.
- 9.5** Armazene a mídia de back-ups em um local seguro fora das instalações, que pode ser tanto uma instalação comercial de armazenamento como um prestador de serviço alternativo.
- 9.6** Exercer a segurança física de toda a mídia de papel e eletrônica (ex: computadores, mídia eletrônica, hardware de rede e comunicação, linhas de telecomunicação, recibos de papel, relatórios em papel e faxes) que contenham informações do portador de cartão.
- 9.7** Mantenha um controle rigoroso sobre a distribuição interna ou externa de qualquer tipo de mídia que contenha informações do portador de cartão
- 9.7.1** Coloque uma etiqueta na mídia de forma que a mesma possa ser identificada como confidencial.
- 9.7.2** Envie a mídia por intermédio de um mensageiro seguro ou um mecanismo de entrega que possa ser acompanhado de forma precisa.
- 9.8** Obtenha a aprovação da administração para qualquer mídia que seja transportada para fora da área de segurança (especialmente quando a mídia for distribuída para indivíduos).
- 9.9** Mantenha um controle rigoroso sobre a armazenagem e acesso à mídia que contenha informações do portador de cartão:
- 9.9.1** Faça um inventário rigoroso de toda a mídia e certifique-se de que a mesma está armazenada de forma segura.
- 9.10** Destrua a mídia contendo as informações do portador de cartão quando não for mais necessária para o negócio ou por razões legais:

9.10.1 Corte no sentido cruzado com picotador de papel, incinere ou reduza à polpa os materiais de cópia física

9.10.2 Purgue, neutralize o campo magnético através do processo de degauss, picote ou destrua de outra forma a mídia eletrônica de maneira a que os dados do portador de cartão não possam ser reconstruídos.

Acompanhe e Teste Regularmente as Redes

Exigência 10: Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão.

Os mecanismos de registro (logs) e a habilidade de acompanhar as atividades do usuário são fundamentais. A presença dos logs em todos os ambientes permite o acompanhamento preciso e a análise quando algo de errado acontece. A determinação da causa de um comprometimento se torna muito difícil sem o registro de atividades.

10.1 Estabeleça um processo para vincular todo o acesso aos componentes do sistema (especialmente aqueles feitos com privilégios administrativos tais como raiz (root) para um usuário individual.

10.2 Implemente os registros de auditoria automatizados para reconstruir os seguintes eventos, para todos os componentes do sistema:

10.2.1 Todo acesso feito por um usuário individual aos dados do portador de cartão

10.2.2 Todas as ações tomadas por qualquer indivíduo com privilégios tipo "root" ou administrativos

10.2.3 Acesso a todos os registros de auditoria

10.2.4 Tentativas de acesso lógico inválidas

10.2.5 Uso de mecanismos de identificação e autenticação

10.2.6 Inicialização dos logs de auditoria

10.2.7 Criação ou eliminação de objetos ao nível de sistema.

10.3 Grave pelo menos os seguintes registros de auditoria para cada evento ligado a todos os componentes do sistema:

10.3.1 Identificação do usuário

10.3.2 Tipo de evento

10.3.3 Data e hora

10.3.4 Indicação de sucesso ou falha

10.3.5 Origem do evento

10.3.6 Identidade ou nome do dado, componente de sistema ou recurso afetado.

10.4 Sincronize todos os relógios e datas de todos os sistemas críticos.

10.5 Torne seguros os registros de auditoria de forma a que eles não possam ser alterados, incluindo o seguinte:

10.5.1 Limite o acesso aos registros de auditoria àqueles que tenham necessidade relacionada com o trabalho

10.5.2 Proteja os arquivos contendo os registros de auditoria contra modificações não autorizadas

10.5.3 Faça o back-up imediato dos arquivos contendo os registros de auditoria em um servidor centralizado de logs ou mídia que seja difícil de alterar

10.5.4 Copie os logs das redes wireless em um servidor de registro na LAN interna.

10.5.5 Use um software de acompanhamento e detecção de mudanças na integridade de arquivos (tal como Tripwire) nos logs de forma a assegurar que os dados dos registros existentes não possam ser alterados sem causar alertas (embora a adição de um novo dado não deva causar um alerta).

10.6 Revise os logs de todos os componentes do sistema pelo menos diariamente. A revisão dos logs deve incluir aqueles servidores que executam funções de segurança tais como IDS e autenticação de servidores (AAA) (ex: RADIUS).

10.7 Mantenha os seus registros de auditoria por um período que seja consistente com o seu uso efetivo, bem como as regulamentações legais.

Um histórico de auditoria geralmente cobre um período de pelo menos um ano, com um mínimo de três meses disponíveis on-line.

Exigência 11: Teste regularmente os sistemas e os processos de segurança

As vulnerabilidades são continuamente descobertas por hackers e pesquisadores ou introduzidas por novos softwares. Os sistemas, processos e softwares customizados devem ser testados freqüentemente para certificar-se de que a segurança está sendo mantida ao longo do tempo e através das mudanças.

11.1 Faça os testes dos controles de segurança, das limitações, das conexões com a rede e das restrições de forma contínua, para certificar-se de que eles podem ser identificados adequadamente ou cancelar quaisquer tentativas de acesso não autorizado. Onde tiver sido instalada a tecnologia de wireless, use um analisador de wireless periodicamente para identificar todos os dispositivos wireless em uso.

11.2 Execute scans para testar a vulnerabilidade interna e externa da rede pelo menos a cada trimestre ou após qualquer mudança significativa na rede (ex: instalação de um novo componente de sistema, mudanças na topologia da rede, modificações na regra do firewall, upgrades de produtos).

Note que os scans de vulnerabilidade externa devem ser executados por um prestador de serviço de scan qualificado pela indústria de cartões de pagamentos.

11.3 Execute um teste de penetração na infraestrutura da rede e aplicativos pelo menos uma vez por ano e após qualquer modificação ou upgrade significativo da infraestrutura ou aplicativo (ex: upgrade do sistema operacional, adição de uma sub-rede no ambiente, adição de um servidor de web no ambiente).

11.4 Use sistemas de detecção de intrusão na rede, sistemas de detecção baseado em host, e/ou sistemas de prevenção de intrusão para acompanhar todo o tráfego na rede e alertar os funcionários para comprometimentos suspeitos. Mantenha atualizados todos os sistemas de detecção e prevenção.

11.5 Instale o acompanhamento da integridade de arquivos para alertar os funcionários sobre uma modificação não autorizada de sistemas críticos ou conteúdo de arquivos e execute as comparações dos arquivos críticos pelo menos diariamente (ou mais freqüentemente se o processo puder ser automatizado).

Os arquivos críticos não são necessariamente aqueles que contêm os dados do portador de cartão. Com relação ao acompanhamento da integridade dos arquivos críticos, são considerados geralmente arquivos críticos aqueles que não

mudam regularmente, mas a modificação pode indicar um comprometimento ou risco de comprometimento do sistema. Os produtos de acompanhamento da integridade de arquivo geralmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, tais como aqueles de aplicativos customizados, devem ser avaliados e definidos pelo estabelecimento ou prestador de serviços.

Mantenha uma Política de Segurança da Informação

Exigência 12: Mantenha uma política que atenda à segurança da informação para funcionários e prestadores de serviços.

Uma política rigorosa de segurança cria um exemplo para toda a empresa e faz com que os funcionários saibam o que é esperado deles. Todos os funcionários devem estar cientes do cuidado a ter com os dados e suas responsabilidades em protegê-los.

- 12.1** Estabeleça, divulgue, mantenha e dissemine uma política de segurança que:
 - 12.1.1** Atenda a todas as exigências contidas nesta especificação
 - 12.1.2** Inclua um processo anual que identifique ameaças e vulnerabilidades e resulte em um levantamento do risco formal
 - 12.1.3** Inclua pelo menos uma revisão anual e updates quando houver mudanças no ambiente
 - 12.2** Desenvolva procedimentos diários de segurança operacional que sejam consistentes com as exigências desta especificação (ex: procedimentos de manutenção da conta do usuário, procedimentos de revisão do log)
 - 12.3** Desenvolva políticas definindo o uso por funcionários que lidam com tecnologias críticas, tais como modems e wireless, para definir o uso apropriado destas tecnologias para todos os funcionários e prestadores de serviços. Certifique-se que estas políticas de uso exijam:
 - 12.3.1** Aprovação explícita pela administração
 - 12.3.2** Autenticação para o uso da tecnologia
 - 12.3.3** Uma lista de todos os dispositivos e funcionários com acesso
 - 12.3.4** Etiquetagem dos dispositivos com indicação do proprietário, informação de contato e objetivo
 - 12.3.5** Uso aceitável da tecnologia
 - 12.3.6** Localização aceitável da rede para estas tecnologias
 - 12.3.7** Uma lista de produtos aprovados pela empresa
 - 12.3.8** Desligamento automático da sessão com modem após um período de inatividade específico
 - 12.3.9** Ativação dos modems para os prestadores de serviço apenas quando for necessário, com imediata desativação após o uso
 - 12.3.10** Desativação da armazenagem de dados do portador de cartão nas unidades de disco locais, floppy disks ou outra mídia externa quando os dados do portador de cartão forem acessados remotamente via modem. Também desativar as funções "cut-and-paste", e "print" durante o acesso remoto
 - 12.4** Assegure-se de que a política de segurança e procedimentos defina claramente as responsabilidades de segurança da informação para todos os funcionários e prestadores de serviço.

12.5 Delegue as seguintes responsabilidades de administração de segurança da informação para um indivíduo ou equipe:

12.5.1 Implementar, documentar e distribuir os procedimentos da política de segurança e regulamentos

12.5.2 Acompanhar e analisar os alertas de segurança e informação e distribuí-los ao pessoal apropriado

12.5.3 Implementar, documentar e distribuir os procedimentos de resposta a um incidente de segurança e escalonamento para assegurar a administração oportuna e eficiente de todas as situações

12.5.4 Administrar as contas dos usuários, incluindo adições, exclusões e modificações

12.5.5 Acompanhar e controlar todo o acesso aos dados.

12.6 Faça com que todos os funcionários estejam cientes da importância atribuída à segurança das informações do portador de cartão

12.6.1 Treinar os funcionários (ex: através de posters, cartas, memorandos, reuniões e promoções).

12.6.2 Exigir que os funcionários reconheçam por escrito que eles leram e entenderam a política e procedimentos de segurança da empresa

12.7 Investigue os funcionários potenciais para minimizar o risco de ataques com origem em fontes internas.

Para aqueles funcionários que apenas possuem acesso a um número de conta de cartão de cada vez para executar uma transação, tais como os caixas das lojas, esta exigência é apenas uma recomendação.

12.8 Exija contratualmente que todos os prestadores de serviço com acesso aos dados do portador de cartão obedeçam às exigências de segurança da indústria de cartões de pagamento. No mínimo, o contrato deve mencionar:

12.8.1 Reconhecimento de que terceiros são responsáveis pela segurança dos dados do portador de cartão em sua posse.

12.8.2 Propriedade por parte de cada marca de cartões de pagamento, Adquirente e Estabelecimentos dos dados do portador de cartão e concordância de que tais dados podem APENAS ser usados para auxiliar estas partes a concluírem uma transação, dando apoio a um programa de lealdade, prestando serviços de controle de fraude ou para outros usos especificamente exigidos por lei.

12.8.3 Continuidade do serviço no evento de um grande distúrbio, desastre ou falha.

12.8.4 Cláusulas de auditorias para assegurar que o representante da indústria de cartões de pagamento, ou um prestador de serviços aprovado pela indústria de cartões de pagamento irá prestar total cooperação e acesso para a condução de uma revisão completa de segurança após um evento de quebra da segurança. A revisão irá validar o atendimento aos padrões da segurança de dados da indústria de cartões de pagamento para a proteção dos dados do portador de cartão.

12.8.5 Cláusula de término do serviço para assegurar que o prestador de serviço irá continuar a tratar como confidencial os dados do portador de cartão.

12.9 Implemente um plano de resposta a um incidente. Esteja preparado para responder imediatamente a uma quebra da segurança do sistema.

12.9.1 Crie um plano de resposta a um incidente para ser usado no evento do comprometimento do sistema. Assegure-se de que o plano atende, pelo menos, aos procedimentos de resposta específicos, processos de recuperação de negócios e continuidade, processos de back-

up dos dados, desempenho e responsabilidades e estratégias de comunicação e contato (ex: informar os Adquirentes e associações de cartões de crédito).

- 12.9.2 Teste o plano pelo menos uma vez por ano.
- 12.9.3 Designe funcionários específicos para estarem disponíveis numa base de 24/7 para responder aos alertas.
- 12.9.4 Faça o treinamento apropriado dos funcionários em termos das responsabilidades pela resposta a uma quebra de segurança.
 - 12.9.5** Inclua alertas originários da detecção de uma intrusão, prevenção de intrusão e sistemas de acompanhamento da integridade dos arquivos.
 - 12.9.6** Crie um processo para modificar e desenvolver o plano de resposta a um incidente de acordo com as lições aprendidas e incorporar os desenvolvimentos da indústria.