



Certificate of PCI DSS Merchant Compliance

Payment Card Industry Data Security Standards Validation

Based on the information provided by the merchant listed below involving its security policies, procedures, and regulations, SecurityMetrics has found the merchant to be compliant with the Payment Card Industry Data Security Standards (PCI DSS), endorsed by Visa, MasterCard, American Express, Discover, and JCB card brands.

ICONE SERVICOS EMPRESARIAIS LTDA

Last Passing Scan Date: 09 Jan 2020

Self Assessment Questionnaire (SAQ C 3.2.1) Compliant Date: 09 Jan 2020

SecurityMetrics recognizes the merchant for its efforts to reduce credit card theft and fraud. By achieving PCI certification, this merchant is maintaining rigorous data security standards to ensure that its customer's credit card information remains safe and secure. In order to maintain PCI DSS compliance the merchant's self-assessment questionnaire must be passed every 12 months and any scans, if applicable, must be passed every 3 months.

www.securitymetrics.com

www.pcisecuritystandards.org

Ian Taylor

Director of Security Fulfillment

Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire C

Merchants with Payment Application Systems Connected to the Internet - No Electronic Cardholder Data Storage

For use with PCI DSS Version 3.2.1
October 2020

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Response		
		Sim	Não	N/A
1.2	As configurações do firewall e do roteador restringem as conexões entre redes não confiáveis e qualquer sistema no ambiente de dados do titular do cartão, da seguinte forma: Observação: uma "rede não confiável" é qualquer rede que seja externa às redes que pertencem à entidade em análise e/ou que esteja além da capacidade da entidade de controlar ou gerenciar.			
1.2.1.a	O tráfego de entrada e saída é restrito ao necessário para o ambiente de dados do titular do cartão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.2.1.b	Todos os outros tráfegos de entrada e saída são recusados de forma específica (como ao usar a opção explícita "recusar todos" ou uma recusa implícita após a declaração de permissão)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.2.3	Existem firewalls de perímetro instalados entre quaisquer redes sem fio e o ambiente de dados do titular do cartão e esses firewalls estão configurados para recusar ou permitir (se esse tráfego for necessário para fins comerciais) apenas tráfegos autorizados a partir do ambiente sem fio no ambiente de dados do titular do cartão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.3	O acesso público direto é proibido entre a internet e qualquer componente do sistema no ambiente de dados do titular do cartão, da seguinte forma:			
1.3.4	O tráfego de saída do ambiente de dados do titular do cartão para a internet está explicitamente autorizado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.3.5	São permitidas apenas as conexões estabelecidas na rede?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Question		Response		
		Sim	Não	N/A
2.1.a	Os valores-padrão entregues pelo fornecedor são sempre alterados antes de instalar um sistema na rede? Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando, às utilizadas pelos sistemas operacionais, softwares que fornecem serviços de segurança, aplicativos e contas do sistema, terminais de ponto de venda (POS), solicitações de pagamento, sequências de comunidade de Protocolo de Gerenciamento de Rede Simples (SNMP), etc).	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.1.b	As contas-padrão desnecessárias são removidas ou desativadas antes da instalação de um sistema na rede?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.1.1	Para ambientes sem fio conectados ao ambiente dos dados do titular do cartão ou para a transmissão dos dados do titular do cartão, TODOS os padrões do fornecedor sem fio são alterados nas instalações, da seguinte forma:			
2.1.1.a	As chaves de criptografia padrão são alteradas na instalação e são modificadas sempre que um funcionário que conhece as chaves sai da empresa ou troca de cargo?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.b	As strings de comunidades de SNMP padrão dos dispositivos sem fio são alteradas na instalação?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.c	As senhas/frases de senha padrão dos pontos de acesso são alteradas na instalação?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.d	O firmware dos dispositivos sem fio é atualizado para ser compatível com a criptografia robusta para autenticação e transmissão em redes sem fio?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1.1.e	Os outros padrões relacionados à segurança do fornecedor de dispositivos sem fio são alterados, se aplicável?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.a	Os padrões de configuração são desenvolvidos para todos os componentes do sistema e estão de acordo com os padrões de fortalecimento do sistema aceitos pelo setor? As fontes para os padrões de fortalecimento do sistema aceitas pelo setor incluem, entre outras, o SysAdmin Audit Network Security (SANS) Institute, o National Institute of Standards Technology (NIST), o International Organization for Standardization (ISO) e o Center for Internet Security (CIS).	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
2.2.b	Os padrões de configuração do sistema são atualizados quando novos problemas de vulnerabilidade são identificados, conforme definido no Requisito 6.1?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.c	Os padrões de configuração do sistema são aplicados quando novos sistemas são configurados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.d	Os padrões de configuração do sistema incluem todos os seguintes itens: * Alteração de todos os padrões informados pelo fornecedor e eliminação de contas padrão desnecessárias? * Implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? * Habilitar apenas serviços, protocolos, daemons, etc. necessários, conforme exigido para a função do sistema? * Recursos de segurança adicionais são implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros? * Os parâmetros de segurança do sistema são configurados para impedir o uso incorreto? * Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores Web desnecessários são removidas?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.1.a	Há a implementação de apenas uma função principal por servidor para evitar funções que exigem diferentes níveis de segurança coexistindo no mesmo servidor? Por exemplo, servidores da Web, servidores do banco de dados e DNS devem ser implementados em servidores separados.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.1.b	e forem usadas tecnologias de virtualização, somente uma função principal está implementada por componente ou dispositivo do sistema virtual?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.2.a	Somente os serviços, protocolos e daemons necessários, entre outros, são ativados conforme a necessidade para a função do sistema (ou seja, os serviços e protocolos que não são diretamente necessários para a execução da função especificada do dispositivo estão desativados)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.2.b	Todos os protocolos, daemons ou serviços não seguros e ativados são justificados de acordo com os padrões de configuração documentados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
2.2.3	Recursos de segurança adicionais são documentados e implantados para todos os serviços, protocolos ou daemons exigidos que são considerados não seguros?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.4.a	Os administradores do sistema e/ou equipes que configuram os componentes do sistema estão bem- informados sobre as configurações comuns dos parâmetros de segurança para esses componentes do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.4.b	As configurações comuns dos parâmetros de segurança estão incluídas nos padrões de configuração do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.4.c	As configurações dos parâmetros de segurança estão definidas corretamente nos componentes do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.5.a	Todas as funcionalidades desnecessárias, como scripts, drivers, recursos, subsistemas, sistemas de arquivo e servidores da web desnecessários foram removidas?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.5.b	As funções ativadas estão documentadas e oferecem suporte para uma configuração segura?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.5.c	Existem somente funcionalidades registradas presentes nos componentes do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.3	Os acessos administrativos fora do console estão criptografados da seguinte forma:			
2.3.a	Todos os acessos administrativos fora do console são criptografados com criptografia robusta e um método de criptografia robusta é invocado antes da solicitação da senha do administrador?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.3.b	Os serviços do sistema e os arquivos de parâmetros são configurados para prevenir o uso de Telnet e outros comandos de login remoto não seguros?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.3.c	O acesso do administrador às interfaces de gerenciamento baseadas na web é criptografado com uma criptografia robusta?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
2.3.d	Para a tecnologia em uso, a criptografia robusta é implementada de acordo com as melhores práticas do setor e/ou recomendações do fornecedor?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.5	Os procedimentos operacionais e as políticas de segurança para gerenciamento dos padrões do fornecedor e outros parâmetros de segurança são/estão: * Documentados * Em uso * Conhecidos por todas as partes envolvidas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Response		
		Sim	Não	N/A
3.2.c	Os dados de autenticação confidenciais são excluídos ou deixados irrecuperáveis ao se completar o processo de autorização?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.d	Todos os sistemas cumprem os seguintes requisitos em relação ao não armazenamento de dados de autenticação confidenciais após a autorização (mesmo se criptografados):			

PCI DSS Question		Response		
		Sim	Não	N/A
3.2.1	<p>O conteúdo completo de qualquer rastreamento (da tarja magnética localizada na parte posterior do cartão ou qualquer dado equivalente presente em um chip ou em qualquer outro lugar) não é armazenado após a autorização?</p> <p>Esses dados também são denominados como rastreamento completo, rastreamento, rastreamento 1, rastreamento 2 e dados da tarja magnética.</p> <p>Observação: no curso normal dos negócios, os seguintes elementos de dados da tarja magnética talvez precisem ser mantidos:</p> <ul style="list-style-type: none"> * O nome do titular do cartão * Número da conta primária (PAN) * Data de vencimento e * Código de serviço <p>Para minimizar o risco, armazene somente os elementos de dados conforme necessário para os negócios.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.2	O código ou valor de verificação do cartão (número de três ou quatro dígitos impresso na frente ou atrás do cartão de pagamento) não é armazenado após a autorização?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Após a autorização, o número de identificação funcionários (PIN) ou o bloqueio de PIN criptografado não é armazenado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.3	<p>O PAN é mascarado quando exibido (os primeiros seis e últimos quatro dígitos são o número máximo de dígitos a serem exibidos) de modo que somente funcionários com uma necessidade comercial legítima podem visualizar mais do que os seis primeiros/últimos quatro dígitos do PAN ?</p> <p>Observação: esse requisito não substitui os requisitos mais rigorosos em vigor quanto às exibições dos dados do titular do cartão, por exemplo, requisitos legais ou da bandeira do cartão de pagamento para recebimentos do ponto de venda (POS).</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question		Response		
		Sim	Não	N/A

PCI DSS Question		Response		
		Sim	Não	N/A
4.1.a	<p>São usados protocolos de segurança e criptografia fortes para proteger dados sensíveis do titular do cartão durante a transmissão através de redes abertas e públicas?</p> <p>Exemplos de redes abertas e públicas incluem, entre outros, internet, tecnologias sem fio, incluindo 802.11 e bluetooth, tecnologias de celular, por exemplo, Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) e General Packet Radio Service (GPRS).</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.b	São aceitas apenas chaves e/ou certificados confiáveis?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.c	São implementados protocolos de segurança para usar apenas configurações seguras e não apoiar versões ou configurações inseguras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.d	É implementada a força da criptografia adequada para a metodologia de encriptação em uso (verificação das recomendações/melhores práticas de fornecedor)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.e	<p>Para implementações de TLS, o TLS é habilitado sempre que dados de titulares de cartão são transmitidos ou recebidos?</p> <p>Por exemplo, para implementações com base no navegador:</p> <p>* O "HTTPS" aparece como parte do protocolo de Universal Record Locator (URL) do navegador, e</p> <p>* Os dados do titular do cartão são exigidos somente se o "HTTPS" aparece como parte do URL.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.1	São usadas as melhores práticas da indústria para implementar criptografia forte para a autenticação e transmissão para as redes sem fio que transmitem dados de titulares de cartão ou que estão conectadas ao ambiente de dados do titular do cartão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.2.b	Existem políticas em vigor que afirmam que os PANs desprotegidos não são enviados por meio das tecnologias de envio de mensagens de usuário final?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
Appendix A2	<p>A2.1 Para terminais POS POI (e os pontos de terminação SSL/TLS ao qual eles se conectam) usando SSL e/ou TLS precoce:</p> <ul style="list-style-type: none"> * Os dispositivos são confirmados para não serem suscetíveis a qualquer falha conhecida para SSL/TLS prematuro * Há um plano formal de redução de riscos e migração em vigor de acordo com a exigência 2.2? <p>A2.2 Existe um plano formal de redução de riscos e migração em vigor para todas as implementações que usam SSL ou TLS precoce (exceto conforme permitido em A2.1), que inclui:</p> <ul style="list-style-type: none"> * Descrição de uso, incluindo dados que estão sendo transmitidos, tipos e número de sistemas que usam e/ou suporte SSL/TLS precoce, tipo de ambiente; * Resultados da avaliação de riscos e controles de redução de risco no lugar; * Descrição dos processos para monitorar as novas vulnerabilidades associadas com SSL/TLS antigo; * Descrição de processos de controle de alterações que são implementados para garantir que o SSL/TLS antigo não seja implementado em novos ambientes; * Visão geral do plano do projeto de migração, incluindo a data de conclusão do objetivo da migração até no máximo 30 de junho de 2018? 			

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Question		Response		
		Sim	Não	N/A
5.1	Os softwares antivírus estão implementados em todos os sistemas normalmente afetados por softwares mal-intencionados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Todos os programas antivírus podem detectar, remover e proteger contra todos os tipos conhecidos de softwares mal-intencionados (como vírus, trojans, worms, spywares, adwares e rootkits)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
5.1.2	São executadas avaliações periódicas para identificar e avaliar a evolução de ameaças de malware a fim de confirmar se tais sistemas continuam sendo considerados como não normalmente afetados por softwares mal-intencionados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.2	Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue:			
5.2.a	Todos os softwares antivírus e as definições são mantidos atualizados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.2.b	As atualizações automáticas e as varreduras periódicas estão ativadas e sendo executadas?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.2.c	Certifique-se de que todos os mecanismos antivírus sejam mantidos conforme segue:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.3	<p>Todos os mecanismos do antivírus:</p> <ul style="list-style-type: none"> * Estão sendo executados ativamente? * Não podem ser desativados ou alterados pelos usuários? <p>Observação: as soluções de antivírus podem ser temporariamente desativadas apenas se houver necessidade técnica comprovada, conforme autorizado pelo gerenciamento com base em cada caso. Se a proteção antivírus precisar ser desativada por um motivo específico, isso deve ser formalmente autorizado. Medidas adicionais de segurança também podem precisar ser implementadas pelo período de tempo durante o qual a proteção antivírus não estiver ativa.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Response		
		Sim	Não	N/A

PCI DSS Question		Response		
		Sim	Não	N/A
6.1	<p>Há um processo para identificar vulnerabilidades de segurança, incluindo o seguinte:</p> <p>* Uso de origens externas conhecidas para obter informações sobre vulnerabilidade?</p> <p>* Classificação de uma escala de risco para as vulnerabilidades, o que inclui identificação de todas as vulnerabilidades de "alto risco" e "críticas"?</p> <p>Observação: as classificações de risco devem ser baseadas nas práticas recomendadas pelo setor, bem como a consideração de impacto potencial. Por exemplo, os critérios para classificar as vulnerabilidades podem incluir a consideração da marca da base CVSS e/ou a classificação pelo fornecedor e/ou os tipos de sistemas afetados.</p> <p>Os métodos para avaliar as vulnerabilidades e classificar o nível de risco variam com base no ambiente da organização e na estratégia de avaliação de risco. As classificações de risco devem, no mínimo, identificar todas as vulnerabilidades consideradas de "alto risco" ao ambiente. Além da classificação de risco, as vulnerabilidades podem ser consideradas "críticas" se apresentarem uma ameaça iminente ao ambiente, sistemas críticos de impacto e/ou resultariam em comprometimento potencial se não resolvidas. Exemplos de sistemas críticos podem incluir sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.2.a	<p>Todos os componentes e softwares do sistema estão protegidos de vulnerabilidades conhecidas devido à instalação de patches de segurança aplicáveis disponibilizados pelo fornecedor?</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.2.b	<p>Os patches de segurança críticos são instalados no prazo de um mês após o lançamento?</p> <p>Observação: os patches de segurança crítica devem ser identificados de acordo com o processo de classificação de risco definido no Requisito 6.1.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.4.6	<p>Após a conclusão de uma mudança significativa, são implementados todos os requisitos do PCI DSS em todos os sistemas novos ou alterados e redes, e é atualizada a documentação conforme aplicável?</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Question		Response		
		Sím	Não	N/A
7.1	O acesso aos componentes do sistema e aos dados do titular do cartão é limitado somente àquelas pessoas cuja função requer tal acesso, conforme itens a seguir:			
7.1.2	O acesso aos IDs de usuários privilegiados é restrito ao seguinte: * Restrito ao menor número de privilégios necessários para o desempenho das responsabilidades da função? * Permitido apenas às funções que requerem especificamente tal acesso privilegiado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.1.3	O acesso é baseado na classificação e na atribuição individual da função da equipe?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Response		
		Sím	Não	N/A
8.1	Há procedimentos e políticas para os controles de gerenciamento de identificação de administradores e usuários que não são clientes em todos os componentes do sistema, conforme a seguir:			
8.1.1	Todos os usuários recebem um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do titular do cartão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.1.5.a	As contas são usadas por terceiros para acessar, suportar ou manter componentes do sistema via acesso remoto habilitado somente durante o período necessário e desativado quando não estiver em uso?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.1.5.b	As contas de acesso remoto de terceiros são monitoradas quando em uso?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
8.1.6.a	Tentativas repetidas de acesso estão limitadas ao bloquear o ID do usuário após seis tentativas, no máximo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.1.7	Após o bloqueio da conta do usuário, a duração do bloqueio está definida para um mínimo de 30 minutos ou até o administrador ativar o ID do usuário?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.1.8	Se uma sessão ficar ociosa por mais de 15 minutos, o usuário é obrigado a se autenticar novamente (informar novamente a senha, por exemplo) para reativar o terminal ou a sessão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2	Além de atribuir um ID exclusivo, um ou mais dos seguintes métodos foi empregado para autenticar todos os usuários? * Algo que você sabe, como uma senha ou frase de senha * Algo que você tem, como um dispositivo de token ou um smart card * Algo que você é, como a biométrica	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2.3.a	Os parâmetros de senha do usuário são configurados para exigir que as senhas/frases de senha atendam ao seguinte? * Exigir um tamanho mínimo de senha de pelo menos sete caracteres * Conter caracteres numéricos e alfabéticos Alternativamente, as senhas/frases secretas devem ter complexidade e força pelo menos equivalentes aos parâmetros especificados acima.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2.4.a	As senhas de usuário/frases secretas são alteradas pelo menos uma vez a cada 90 dias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2.5.a	Um indivíduo deve criar uma nova senha/frase secreta diferente das últimas quatro senhas/frases de senha usadas?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2.6	As senhas/frases secretas são definidas com um valor exclusivo para cada usuário para a primeira utilização e após reiniciar, e cada usuário deve mudar sua senha imediatamente após o primeiro uso?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
8.3	<p>Todo acesso administrativo individual que não utiliza console e todo acesso remoto ao CDE é protegido usando a autenticação multifatores, conforme a seguir?</p> <p>Observação: a autenticação multifatores exige que um mínimo de dois dos três métodos de autenticação (ver Exigência 8.2 de PCI DSS para obter descrições dos métodos de autenticação) seja usado para autenticação. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado como autenticação multifatorial.</p>			
8.3.1	É incorporada autenticação multifatores para todos os acessos que não utilizam console no CDE para os funcionários com acesso administrativo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.3.2	É incorporada autenticação multifatores em todos os acessos de rede remota (usuário e administrador e incluindo o acesso de terceiros para suporte ou manutenção) provenientes de fora da rede da entidade?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.4.a	Os procedimentos e políticas de autenticação são documentados e comunicados a todos os usuários?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.4.b	<p>Os procedimentos e políticas de autenticação incluem o seguinte?</p> <p>* Orientação sobre selecionar credenciais fortes de autenticação</p> <p>* Orientação sobre como os usuários devem proteger suas credenciais de autenticação</p> <p>* Instruções para não reutilizar senhas anteriormente usadas</p> <p>* Instruções para os usuários de alteração da senha se houver suspeita de que ela possa estar comprometida</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5	<p>As contas e senhas (ou outros métodos de autenticação) de grupo, compartilhadas ou genéricas, são proibidas conforme os itens a seguir:</p> <p>* Os IDs e as contas de usuários genéricos são desativados ou removidos;</p> <p>* Não existem IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas; e</p> <p>* IDs de usuários compartilhados e genéricos não são usados para administrar quaisquer componentes do sistema?</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
8.8	<p>Os procedimentos operacionais e políticas de segurança para a identificação e autenticação são/estão:</p> <ul style="list-style-type: none"> * Documentados * Em uso * Conhecidos por todas as partes envolvidas 	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response		
		Sim	Não	N/A
9.1	Existem controles adequados em vigor para a entrada na instalação para limitar e monitorar o acesso físico aos sistemas no ambiente de dados do titular do cartão?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.1.1.a	<p>Existem câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) para monitorar o acesso físico individual em áreas sensíveis?</p> <p>Observação: "áreas confidenciais" referem-se a qualquer central de dados, sala de servidores ou qualquer área que contenha sistemas que armazenem, processem ou transmitam dados do titular do cartão. Isso exclui áreas voltadas ao público, onde apenas os terminais de ponto de venda estão presentes como as áreas de caixa em uma loja de varejo.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.1.1.b	As câmeras de vídeo ou mecanismos de controle de acesso (ou ambos) são protegidos contra adulteração ou desabilitação?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.1.1.c	Os dados são coletados a partir de câmeras de vídeo e/ou mecanismos de controle de acesso revisados e correlacionados com outras entradas?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.1.1.d	Os dados são coletados de câmeras de vídeo e/ou mecanismos de controle de acesso armazenados por pelo menos três meses, menos em caso contrário restrito por lei?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

PCI DSS Question		Response		
		Sim	Não	N/A
9.1.2	<p>Os controles físicos e/ou lógicos são usados para restringir o acesso a pontos de rede acessíveis publicamente?</p> <p>Por exemplo, pontos de rede localizados em áreas públicas e áreas acessíveis a visitantes podem ser desativados e somente ativados quando o acesso à rede é explicitamente autorizado. Alternativamente, processos podem ser implementados para garantir que os visitantes sempre sejam acompanhados nas áreas com pontos de rede ativos.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
9.5	<p>Todas as mídias estão fisicamente seguras (incluindo, entre outros, computadores, mídias eletrônicas removíveis, recibos em papel, relatórios em papel e faxes)?</p> <p>Para os fins do requisito 9, "mídia" refere-se a todas as mídias em papel ou eletrônicas que contêm dados do titular do cartão.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.6.a	É mantido um controle rigoroso quanto à distribuição interna ou externa de qualquer tipo de mídia?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.6.b	Os controles incluem o seguinte:			
9.6.1	A mídia é classificada para que a confidencialidade dos dados possa ser determinada?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.6.2	A mídia é enviada via um mensageiro seguro ou outro método de entrega que possa ser rastreado com precisão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.6.3	A aprovação gerencial é obtida antes de mover as mídias (especialmente quando a mídia é distribuída a pessoas)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.7	É mantido um controle rigoroso sobre o armazenamento e a acessibilidade das mídias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.8.a	Todas as mídias são destruídas quando não são mais necessárias por razões corporativas ou legais?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.8.c	A destruição é executada da seguinte forma:			
9.8.1.a	Os materiais impressos são fragmentados, incinerados ou reciclados, de forma que os dados do titular do cartão não possam ser reconstruídos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
9.8.1.b	Os contêineres usados para materiais que armazenam informações são destruídos de forma segura para prevenir o acesso aos conteúdos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9	Os dispositivos que capturam os dados do cartão de pagamento por meio de interação física direta com o cartão são protegidos contra falsificação e substituição conforme a seguir? Observação: esse requisito é aplicável aos dispositivos de leitura do cartão usados em transações com a presença do cartão (ou seja, de passar ou inserir) no ponto de venda. Este requisito não tem o objetivo de se aplicar aos componentes de entrada de chave manual, como teclados de computador e teclados POS.			
9.9.a	As políticas e procedimentos exigem que uma lista de tais dispositivos seja mantida?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.b	As políticas e procedimentos exigem que os dispositivos sejam periodicamente inspecionados quanto à falsificação ou substituição?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.c	As políticas e procedimentos exigem que os funcionários sejam treinados para reconhecer os comportamentos suspeitos e reportar a falsificação ou substituição de dispositivos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.1.a	A lista de dispositivos inclui o seguinte? * Marca, modelo do dispositivo * Localização do dispositivo (por exemplo, o endereço do local ou instalação onde o dispositivo está localizado) * Número de série do dispositivo ou outro método de identificação exclusivo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.1.b	Essa lista é precisa e está atualizada?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.1.c	Essa lista de dispositivos é atualizada quando dispositivos são adicionados, realocados, retirados de serviço etc?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
9.9.2.a	<p>As superfícies dos dispositivos são inspecionadas periodicamente para detectar falsificação (por exemplo, adição de espíões aos dispositivos) ou substituição (por exemplo, verificando o número de série ou outras características do dispositivo para verificar se ele não foi trocado por um dispositivo fraudulento) como segue?</p> <p>Observação: exemplos de sinais de que um dispositivo possa ter sido adulterado ou substituído incluem apêndices inesperados ou cabos conectados ao dispositivo, rótulos de segurança alterados ou ausentes, revestimento quebrado ou de cor diferente, ou alterações no número de série ou outras marcas externas.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.2.b	Os funcionários estão cientes dos procedimentos de inspeção dos dispositivos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.3	Os funcionários são treinados para reconhecer tentativas de falsificação ou substituição de dispositivos para incluir o seguinte?			
9.9.3.a	<p>Os materiais de treinamento para os funcionários nos locais dos pontos de venda incluem o seguinte?</p> <p>* Verifique a identidade de qualquer terceiro que alegue ser da equipe de manutenção ou reparo, antes de conceder acesso para modificar ou resolver problemas nos dispositivos. * Não instale, substitua ou devolva dispositivos sem verificação. * Esteja atento a comportamentos suspeitos ao redor dos dispositivos (por exemplo, tentativas de desconectar ou abrir os dispositivos por pessoas desconhecidas). * Reporte comportamentos suspeitos e indicações de adulteração ou substituição para a equipe apropriada (por exemplo, para um gerente ou funcionário da segurança).</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.3.b	Os funcionários dos locais dos pontos de venda recebem treinamento e conhecem os procedimentos para detectar e reportar tentativas de falsificação ou substituição de dispositivos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Question		Response		
		Sim	Não	N/A
10.2	Foram implementadas trilhas de auditoria automatizadas para todos os componentes do sistema para recuperar os seguintes eventos:			
10.2.2	Todas as ações desempenhadas por qualquer pessoa com privilégios raiz ou administrativos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Tentativas inválidas de acesso lógico?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Há uso e alterações dos mecanismos de identificação e autenticação, incluindo, entre outros, a criação de novas contas e aumento de privilégios e todas as alterações, adições ou exclusões de contas com privilégios raiz ou administrativos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3	As seguintes entradas da trilha de auditoria são registradas para todos os componentes do sistema em cada um dos eventos a seguir?			
10.3.1	Identificação do usuário?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Tipo de evento?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Data e hora?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Indicação de sucesso ou falha?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origem do evento?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identidade ou nome dos dados, componentes do sistema ou recursos afetados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.6	Os logs e ocorrências de segurança para todos os componentes do sistema são revisados para identificar irregularidades ou atividades suspeitas conforme a seguir? Observação: as ferramentas de coleta, análise e alerta dos registros podem ser usadas para estar em conformidade com o Requisito 10.6			

PCI DSS Question		Response		
		Sim	Não	N/A
10.6.1.b	Os eventos de segurança e registros são analisados ao menos diariamente? * Todas as ocorrências de segurança * Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD * Logs de todos os componentes críticos do sistema * Logs de todos os servidores e componentes do sistema que desempenham funções de segurança (por exemplo, firewalls, sistemas de detecção de invasão/sistemas de prevenção contra invasão (IDS/IPS), servidores de autenticação, servidores de redirecionamento do comércio eletrônico, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.6.2.b	Análises de todos os outros componentes do sistema são executadas de acordo com a política e a estratégia de gerenciamento de risco da organização?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.6.3.b	É executado um acompanhamento das exceções e anomalias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.7.b	Os logs de auditoria são retidos pelo menos uma vez ao ano?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.7.c	Ao menos os últimos três meses de logs estão imediatamente disponíveis para análise?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Response		
		Sim	Não	N/A
11.1.a	Processos para detecção e identificação dos pontos de acesso sem fio não autorizados e autorizados são implementados trimestralmente? Observação: métodos que podem ser usados no processo incluem, entre outros, varreduras de rede sem fio, inspeções físicas/lógicas de componentes e infraestrutura do sistema, controle de acesso à rede (NAC) ou IDS/IPS sem fio. Qualquer método usado deve ser suficiente para detectar e identificar qualquer dispositivo não autorizado.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

PCI DSS Question		Response		
		Sim	Não	N/A
11.1.b	<p>A metodologia detecta e identifica qualquer ponto de acesso sem fio não autorizado, incluindo ao menos os itens a seguir?</p> <p>* Cartões WLAN inseridos nos componentes do sistema; * Dispositivos móveis ou portáteis fixados a componentes do sistema para criar um ponto de acesso sem fio (por exemplo, por USB, etc.); e * Dispositivos sem fio conectados a uma porta de rede ou a um dispositivo de rede.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.1.c	Se a varredura sem fio for utilizada para identificar os pontos de acesso sem fio autorizados e não autorizados, a varredura é executada pelo menos trimestralmente para todos os componentes e instalações do sistema?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.1.d	Se o monitoramento automatizado for utilizado (como IDS/IPS sem fio, NAC etc.), ele está configurado para gerar alertas à equipe?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.1.1	Um inventário de pontos de acesso sem fio autorizados é mantido e uma justificativa comercial é documentada para todos os pontos de acesso sem fio autorizados?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.1.2.a	O plano de resposta a incidentes define e exige uma resposta em caso de detecção de ponto de acesso sem fio não autorizado?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.1.2.b	São tomadas ações quando os pontos de acesso sem fio não autorizados são encontrados?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

PCI DSS Question		Response		
		Sim	Não	N/A
11.2	<p>São executadas varreduras das vulnerabilidades das redes internas e externas pelo menos trimestralmente e após qualquer alteração significativa na rede (como instalações de novos componentes do sistema, alterações na topologia da rede, modificações das normas do firewall, upgrades de produtos) da seguinte forma:</p> <p>Observação: vários relatórios de varredura podem ser combinados no processo de varredura trimestral para mostrar que todos os sistemas foram mapeados e que todas as vulnerabilidades aplicáveis foram resolvidas. Pode ser exigida uma documentação adicional para verificar se as vulnerabilidades não resolvidas estão em processo de serem solucionadas.</p> <p>Para a conformidade inicial com o PCI DSS, não é necessário que as quatro varreduras trimestrais aprovadas sejam concluídas se o assessor verificar que 1) o resultado da varredura mais recente foi uma varredura aprovada, 2) a entidade possui políticas e procedimentos documentados que requerem a sequência de varreduras trimestrais e 3) as vulnerabilidades observadas nos resultados da varredura tenham sido corrigidas conforme mostrado em uma nova varredura. Nos anos seguintes após a análise inicial do PCI DSS, quatro varreduras trimestrais aprovadas devem ter ocorrido.</p>			
11.2.1.a	As varreduras das vulnerabilidades internas são executadas trimestralmente?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.1.b	O processo de varredura interna trimestral trata todas as vulnerabilidades de "alto risco" e inclui novas varreduras para verificar se todas as vulnerabilidades de "alto risco" (conforme definido pela Exigência 6.1 de PCI DSS) são resolvidas?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.1.c	As varreduras são executadas trimestralmente por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

PCI DSS Question		Response		
		Sim	Não	N/A
11.2.2.a	<p>As varreduras das vulnerabilidades externas são executadas trimestralmente?</p> <p>Observação: as varreduras externas trimestrais de vulnerabilidades devem ser realizadas por um Fornecedor de Varreduras Aprovado (ASV) qualificado pelo Conselho de padrões de segurança da indústria de cartões de pagamento (PCI SSC).</p> <p>Consulte o Guia do programa ASV publicado no site do PCI SSC para saber sobre responsabilidades de varredura do cliente, preparação de varredura, etc.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.2.b	Os resultados da varredura externa trimestral cumprem os requisitos do Guia do programa ASV (por exemplo, nenhuma vulnerabilidade classificada com valor 4 ou superior pelo CVSS e nenhuma falha automática)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.2.c	As varreduras de vulnerabilidades externas trimestrais são executadas por um fornecedor de varredura aprovado (ASV) pela PCI SSC?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.3.a	<p>Varreduras internas e externas e novas varreduras são realizadas, se necessário, após qualquer mudança significativa?</p> <p>Observação: As varreduras devem ser realizadas por uma equipe qualificada.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.3.b	<p>O processo de varredura inclui novas varreduras até que:</p> <p>* Não existam vulnerabilidades com pontuação de 4 ou mais pelo CVSS para varreduras externas</p> <p>* Um resultado aprovado seja obtido ou todas as vulnerabilidades definidas como "alto risco", conforme definido no Requisito 6.1 do PCI DSS, estejam solucionadas (para varreduras internas)?</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.2.3.c	As varreduras são executadas por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.3.4	Se a segmentação é usada para isolar o CDE de outras redes:			

PCI DSS Question		Response		
		Sim	Não	N/A
11.3.4.a	Os procedimentos de testes de penetração são definidos para testar todos os métodos de segmentação, para confirmar que eles estão operacionais e eficazes e isolam todos os sistemas fora de escopo dos sistemas no CDE?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.3.4.b	<p>O teste de penetração para verificar os controles de segmentação atendem ao seguinte?</p> <p>* É executado pelo menos uma vez ao ano e após qualquer mudança nos métodos/controles da segmentação</p> <p>* Abrange todos os métodos/controles da segmentação em uso</p> <p>* Verifica se os métodos de segmentação estão operacionais e eficientes e isola todos os sistemas fora de escopo dos sistemas no CDE</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.3.4.c	Os testes são executados por um recurso interno qualificado ou um terceiro externo qualificado e, caso aplicável, há uma independência organizacional do responsável pelo teste (não é necessário que seja um QSA ou ASV)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.5.a	<p>Existe um mecanismo de detecção de mudança (por exemplo, ferramentas de monitoramento de integridade de arquivo) implementado para detectar modificações não autorizadas (incluindo as alterações, adições e exclusões) de arquivos críticos de sistema, arquivos de configuração ou arquivos de conteúdo?</p> <p>Os exemplos de arquivos que devem ser monitorados incluem:</p> <p>* Executáveis do sistema</p> <p>* Executáveis dos aplicativos</p> <p>* Arquivos de configuração e parâmetro</p> <p>* Arquivos de log e auditoria, históricos ou arquivados, armazenados centralmente</p> <p>* Arquivos críticos adicionais determinados pela entidade (por exemplo, por meio de avaliação de risco ou outros meios)</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

PCI DSS Question		Response		
		Sim	Não	N/A
11.5.b	<p>O mecanismo de detecção de mudança é configurado para alertar os funcionários sobre modificação não autorizada (incluindo as alterações, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo, e as ferramentas realizam comparações de arquivos críticos pelo menos semanalmente?</p> <p>Observação: para fins de detecção de alterações, os arquivos críticos normalmente são aqueles que não são alterados com frequência, mas sua modificação poderia indicar um comprometimento do sistema ou um risco de comprometimento. Os mecanismos de detecção de alterações, como produtos de monitoramento da integridade dos arquivos, normalmente vêm pré-configurados com arquivos críticos para o sistema operacional relacionado. Outros arquivos críticos, como aqueles para os aplicativos personalizados, devem ser avaliados e definidos pela entidade (ou seja, o comerciante ou prestador de serviços).</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
11.5.1	Há um processo implementado para responder a qualquer alerta gerado pela solução de detecção de alterações?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Question		Response		
		Sim	Não	N/A
12.1	Existe uma política de segurança estabelecida, publicada, mantida e disseminada para todas as equipes relevantes?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.1.1	A política de segurança é revisada ao menos uma vez por ano e atualizada quando o ambiente é alterado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3	<p>O uso de políticas de tecnologias críticas é desenvolvido para definir o uso apropriado destas tecnologias e exige o seguinte:</p> <p>Observação: exemplos de tecnologias críticas incluem, entre outros, tecnologias de acesso remoto e sem fio, laptops, tablets, mídia eletrônica removível, uso de e-mails e da internet.</p>			

PCI DSS Question		Response		
		Sim	Não	N/A
12.3.1	Aprovação explícita pelas partes autorizadas para uso das tecnologias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Autenticação para o uso da tecnologia?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.3	Uma lista de todos esses dispositivos e equipes com acesso?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Usos aceitáveis das tecnologias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Locais de rede aceitáveis para as tecnologias?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Desconexão automática das sessões para tecnologias de acesso remoto após um período específico de inatividade?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Ativação de tecnologias de acesso remoto para fornecedores e parceiros de negócio somente quando lhes for necessário, com desativação imediata após o uso?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.4	A política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança das informações para todas as equipes?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5.b	As seguintes responsabilidades de gerenciamento da segurança da informação são atribuídas formalmente para as pessoas e equipes que:			
12.5.3	Estabelecem, documentam e distribuem procedimentos de resposta e escalção de incidentes de segurança para assegurar que todas as situações sejam abordadas de modo oportuno e eficiente?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.6.a	Existe um programa de conscientização de segurança formal para tornar todos os funcionários conscientes da política e dos procedimentos de segurança dos dados dos titulares de cartão?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8	As políticas e procedimentos são mantidos e implementados para gerenciar os prestadores de serviços com os quais os dados do titular do cartão são compartilhados, ou que possam afetar a segurança dos dados, conforme segue:			
12.8.1	É mantida uma lista dos prestadores de serviços, incluindo uma descrição dos serviços prestados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
12.8.2	<p>É mantido um acordo por escrito que inclua um reconhecimento de que os prestadores de serviços são responsáveis pela segurança dos dados que possuem do titular do cartão, ou que os armazenam, processam ou transmitem em nome do cliente, ou ao ponto de que eles possam impactar a segurança do ambiente dos dados do titular do cartão do cliente?</p> <p>Observação: as informações exatas contidas no reconhecimento dependerão do acordo entre as duas partes, dos detalhes do serviço a ser prestado e das responsabilidades atribuídas a cada parte. O reconhecimento não precisa ser exatamente igual ao fornecido neste requisito.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.3	Existe um processo definido para a contratação dos prestadores de serviços, incluindo uma diligência devida adequada antes da contratação?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.4	É mantido um programa para monitorar anualmente o status de conformidade com o PCI DSS dos prestadores de serviços?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.5	As informações mantidas sobre os requisitos do PCI DSS são administradas por cada prestador de serviços e quais são administradas pela entidade?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.a	Foi criado um plano de resposta a incidentes para ser implementado em caso de violação do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b	No mínimo, o plano aborda o seguinte:			
12.10.1.b.1	Funções, responsabilidades e estratégias de comunicação e contato no caso de um comprometimento, incluindo, no mínimo, a notificação às bandeiras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b.2	Procedimentos de resposta específicos a incidentes?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b.3	Procedimentos de recuperação e continuidade dos negócios?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b.4	Processos de backup dos dados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b.5	Análise dos requisitos legais para divulgação dos comprometimentos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Question		Response		
		Sim	Não	N/A
12.10.1.b.6	Abrangência e respostas de todos os componentes críticos do sistema?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.10.1.b.7	Referência ou inclusão de procedimentos de resposta a incidentes por parte das bandeiras?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	