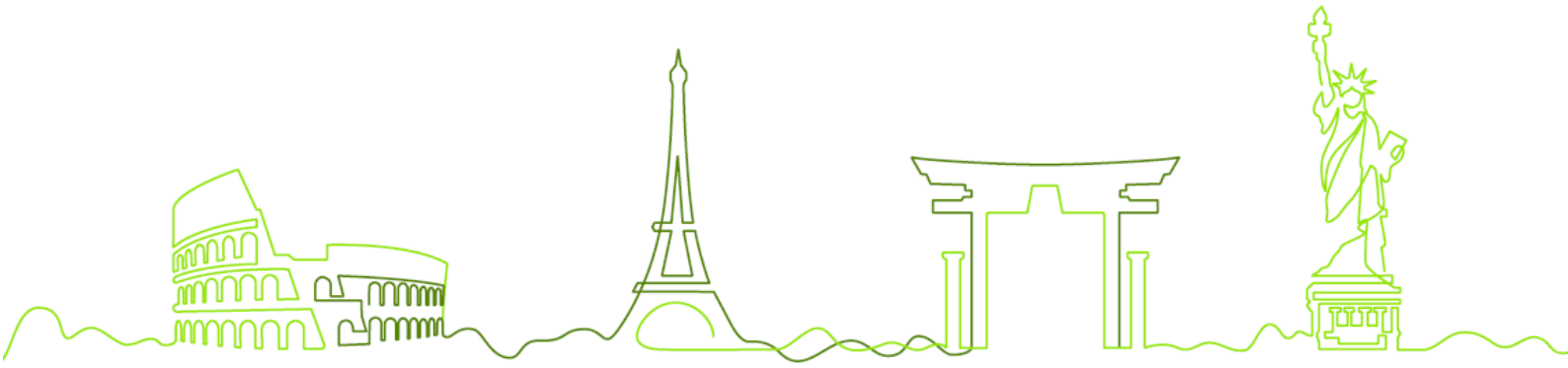

Política PCI-DSS

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	30 abr 2025	Cibersegurança	Versão Original

Sumário

1. Objetivo

A finalidade deste documento é estabelecer processos, procedimentos e padrões que devem ser seguidos para proteger os dados do titular do cartão (CHD) e os sistemas, de acordo com o padrão de segurança de dados do setor de cartões de pagamento (PCI DSS). Ele deve ser usado pela equipe de tecnologia da informação e operações do Intex Bank Banco de Câmbio S/A, referenciada abaixo somente como “Intex Bank”, durante a gestão dos dados e processos.

2. Escopo

Este documento se aplica a todos os usuários e sistemas gerenciados pelo “Intex Bank” que armazenam, processam, transmitem, visualizam ou afetam a segurança dos dados do titular do cartão. Todos os funcionários que alteram ou realizam manutenção em tais sistemas devem aderir às políticas e aos procedimentos contidos neste documento.

Esta Política se aplica a todos os funcionários do “Intex Bank” e a todas as partes externas com acesso a redes de produção e recursos de sistema relacionados aos dados do titular do cartão e/ou ao ambiente de dados do titular do cartão.

Esta política está alinhada com o PCI DSS, norma internacional essencial para a segurança das transações envolvendo dados de titulares de cartão, bem como com a Resolução CMN nº 4.893/2021 e a Resolução BCB nº 85/2021, que estabelecem exigências para a estrutura de segurança cibernética e a gestão de riscos operacionais e de incidentes em instituições financeiras. A política também adota boas práticas do NIST Cybersecurity Framework (CSF) e da ISO/IEC 27001:2022, que orientam a implementação de controles técnicos e administrativos de segurança da informação. Além disso, reforça a conformidade com a LGPD (Lei nº 13.709/2018), no que tange à proteção de dados pessoais sensíveis, e com a Lei nº 9.613/1998, ao estabelecer medidas que contribuem para a prevenção à lavagem de dinheiro, especialmente pela rastreabilidade e proteção dos dados financeiros processados.

3. Política

A proteção dos dados do titular do cartão e das pessoas, processos e tecnologias relacionados ao ambiente de dados do titular do cartão é um requisito obrigatório do setor. Como comerciante que lida com dados do titular do cartão, o “Intex Bank” deve estar em conformidade com todos os aspectos do padrão de segurança de dados PCI; o não cumprimento dos padrões de segurança pode levar a riscos para o “Intex Bank”, incluindo

multas significativas, violações e riscos negativos para a reputação da organização.
O conteúdo a seguir são especificações para o ambiente de cartões de pagamento do "Intex Bank" e destinam-se a complementar as políticas e os procedimentos existentes.

4. Padrões de Tratamento de Dados de Titulares de Cartões

Os requisitos a seguir são aplicáveis a todos os dados do titular do cartão (CHD) armazenados ou processados nos sistemas do "Intex Bank":

a) O CHD nunca poderá ser armazenado em nenhum sistema do "Intex Bank" por qualquer motivo; ou

b) O armazenamento e a retenção do CHD não podem exceder o exigido por requisitos legais, regulamentares e/ou comerciais, conforme especificado na Política de Gestão, Classificação e Proteção da Informação.

c) Os dados do titular do cartão devem ser excluídos ou removidos com segurança quando não forem mais necessários por motivos legais, regulamentares ou comerciais, conforme especificado na Política de Gestão, Classificação e Proteção da Informação.

d) Com frequência **trimestral**, o "Intex Bank" deverá remover com segurança os CHD que excedem os requisitos de retenção, executando o definido na Política de Gestão, Classificação e Proteção da Informação.

e) É proibido armazenar dados de autenticação confidenciais (SAD) após a autorização ou gravar esses dados em disco (como logs ou armazenamento em mídia impressa); isso inclui o código de verificação do cartão de três ou quatro dígitos ou o valor impresso na frente do cartão ou painel de assinatura (dados de CVV2, CVC2, CID, CAV2), dados completos de faixa/tarja magnética ou dados equivalentes de faixa, número de identificação pessoal (PIN) ou bloqueio de PIN criptografado. Os SAD nunca podem ser armazenados em qualquer formato após a autorização (3.3.1), e os SAD armazenados temporariamente antes da autorização devem ser protegidos com criptografia forte de acordo com padrões de criptografia documentados e aprovados (3.3.2).

f) A criptografia em nível de disco ou partição (em vez de criptografia de banco de dados em nível de arquivo, coluna ou campo) somente pode ser usada para proteger mídias eletrônicas removíveis; o PAN armazenado em qualquer mídia (como disco ou mídia eletrônica não removível) também deve ser tornado ilegível usando um mecanismo de proteção secundário aprovado, de acordo com o requisito 3.5.1 do

PCI DSS.

g) Nenhuma pessoa está autorizada a ver o número da conta principal (PAN) por qualquer motivo; ou.

h) O número da conta primária (PAN) completo deve ser mascarado para os primeiros 6 ou últimos 4 dígitos quando exibido em qualquer sistema, a menos que um usuário tenha uma necessidade comercial válida para ver o número da conta completo (3.4.1). As funções aprovadas a seguir são as únicas autorizadas a ver o PAN completo:

Função	Finalidade comercial
Atendimento ao Cliente	Pode ver um único PAN completo de cada vez para atualizações de pedidos e faturamento.
Fraude/LP	Pode ver o PAN completo para investigar fraudes.
Equipe de Finanças	Pode ver o PAN completo para concluir o faturamento ou resolver problemas contábeis.

i) Qualquer CHD armazenado nos sistemas do "Intex Bank" deve ser protegido usando criptografia simétrica utilizando o algoritmo AES (Advanced Encryption Standard) com chaves de 256 bits, configurada para expirar e ser substituída em um intervalo máximo de 1 (um) ano. de acordo com a Política de Criptografia.

j) Quando os hashes forem usados para tornar o PAN ilegível, deverão ser usados hashes criptográficos com chave de todo o PAN, com processos e procedimentos de gerenciamento de chaves associados, de acordo com os Requisitos 3.6 e 3.7.

k) Ao acessar os sistemas do CHD, todos os funcionários estão proibidos de copiar, mover e armazenar dados do titular do cartão em sistemas não autorizados (p. ex: discos rígidos locais e mídia eletrônica removível), a menos que explicitamente autorizado pela gerência para atender a uma necessidade comercial específica, e os controles técnicos devem impedir a cópia e/ou a realocação do PAN para todos os funcionários, exceto para quem tiver autorização documentada e explícita e uma necessidade comercial legítima e definida (3.4.2).

l) Os colaboradores com acesso aos dados e sistemas do titular do cartão (como funcionários e contratados) devem proteger todos os dados do titular do cartão de acordo com os Requisitos do PCI DSS (3.4.2).

m) Todos os funcionários com acesso direto ao CHD devem passar pelo treinamento **anual** para garantir que estejam cientes de suas responsabilidades de proteger os dados e sistemas do titular do cartão (12.6).

n) As credenciais de CHD e de autenticação enviadas por redes abertas e públicas, incluindo redes sem fio, exigem o uso de criptografia forte, como SSH, TLS 1.1 ou superior, ou HTTPS que use cifras fortes de acordo com a Política de Criptografia. Protocolos inseguros, como TLS inicial, SSL, WEP, entre outros, devem ser desativados (4.2).

o) É proibido enviar CHD, incluindo PAN, por qualquer canal não autorizado, incluindo tecnologias de mensagens para usuários finais (chat, texto, SMS, e-mail etc.) (4.2.1, 4.2.2).

p) Os sistemas comumente afetados por malware que armazenam, processam, transmitem ou se conectam a sistemas que afetam as redes de dados do titular do cartão devem ter o software antimalware apropriado ativado e configurado de acordo com os padrões de antivírus descritos na Política de Segurança da Informação. Isso inclui a configuração do software antimalware para detectar, remover e/ou colocar em quarentena automaticamente softwares e arquivos mal-intencionados por meio de varredura periódica ou análise comportamental contínua de sistemas e processos. Os mecanismos e as definições de antimalware devem ser mantidos atualizados o tempo todo e devem incluir cobertura para mídia eletrônica removível. (5.3).

q) O "Intex Bank" analisará a necessidade de antimalware para todos os sistemas que não precisem dele (por exemplo, que não são comumente afetados por software malicioso) periodicamente por meio do processo de avaliação de risco **anual** (5.2.1) (5.2.3) (5.2.3.1).

r) Os registros de eventos de software antimalware devem ser mantidos por um ano, com três meses disponíveis para análise imediata (5.3.4) (10.7)

5. Controle de Acesso

O acesso ao CHD e aos sistemas deve ser concedido com base nos princípios do privilégio mínimo e função/cargo. Todo acesso ao CHD e aos sistemas deve seguir os procedimentos de gerenciamento de mudanças e autorização, conforme especificado na Política de

Controle de Acesso, e todo acesso requer aprovação explícita da gerência ou dos proprietários autorizados de dados e sistemas.

A seguir estão descritos os requisitos mínimos para controlar o acesso ao CHD e aos sistemas:

a) Todos os usuários precisam de um ID exclusivo para acessar os componentes do sistema ou os dados do titular do cartão (8.2.1). Onde um ID exclusivo não pode ser usado:
- O uso da conta é impedido fora de circunstâncias excepcionais;
- O uso é limitado apenas ao tempo necessário para a circunstância excepcional;
- A justificativa e o uso comercial são explicitamente documentados e aprovados pela gerência;
- A identidade do usuário individual é confirmada antes de conceder acesso à conta;
- Cada ação realizada é atribuível a um usuário individual (como o usuário ao qual foi concedido acesso).

b) Além de um ID exclusivo, todo o acesso deve empregar pelo menos um dos seguintes métodos (8.3.1):
- Algo que você conhece, como uma senha ou frase secreta;
- Algo que você possui, como um token ou cartão inteligente;
- Algo que você é, como um elemento biométrico;

c) A adição, exclusão e modificação de IDs de usuário, credenciais e outros objetos identificadores devem seguir todos os procedimentos de acesso definidos na Política de Controle de Acessos;

d) O acesso deve ser revogado imediatamente para todos os usuários demitidos (8.2.5);

e) As contas de usuário inativas/expiradas com acesso ao CHD e aos sistemas devem ser identificadas e removidas pelo menos a cada 90 dias (8.2.6);

f) Os fornecedores que acessam, oferecem suporte ou mantêm componentes do sistema CHD por meio de acesso remoto devem ter seu acesso ativo somente durante o período necessário e desativado quando não estiverem em uso. O acesso e as ações do fornecedor devem ser monitorados quando a conta estiver em uso. (8.2.7);

g) As contas com acesso ao CHD e aos sistemas deverão ser bloqueadas após, no máximo, 10 (dez) tentativas de acesso malsucedidas, com uma duração de bloqueio de, no mínimo, 30 minutos ou até que um administrador habilite o ID de usuário após validar a identidade do usuário; (8.3.4)

h) As sessões nos sistemas CHD exigem que o usuário se autentique novamente para reativar o terminal ou a sessão após no máximo, 15 minutos de inatividade (8.2.8);

i) Senhas e outros mecanismos de autenticação devem empregar o uso de criptografia forte ou hashing durante o armazenamento ou transmissão (8.3.2);

j) A redefinição/alteração remota de uma credencial de autenticação (por exemplo, por telefone, e-mail, web ou outro método não presencial) exige a verificação da identidade do usuário antes da redefinição (8.3.3);

k) As configurações de senha devem ser definidas com segurança, conforme definido na Política de Segurança da Informação.

l) Todos os usuários devem seguir as práticas recomendadas para proteger, reutilizar, escolher e alterar senhas, conforme definido na Política de Controle de Acessos. Isso inclui o seguinte:

- Desativar/remover IDs e contas de usuários genéricos.
- Desativar/remover IDs de usuários compartilhados para atividades de administração do sistema e outras funções críticas.
- Quando o MFA não for usado, as senhas/frases secretas serão alternadas a cada 90 dias, e a postura de segurança da conta será monitorada dinamicamente e o acesso aos recursos será determinado com base nos resultados desse monitoramento.
- Selecionar e usar somente senhas fortes que não sejam fáceis de adivinhar (por exemplo, Password123!, Spring2023?)
- Com um mínimo de 12 caracteres alfanuméricos sempre que possível e 8 quando não for possível
- Que não seja nenhuma das últimas duas senhas usadas

m) As contas de grupo, compartilhadas ou genéricas, ou outras credenciais de autenticação compartilhadas, são usadas somente quando necessário, em caráter excepcional, e são gerenciadas da seguinte forma (8.2.2):

- O uso da conta é impedido, a menos que seja necessário para uma circunstância excepcional.
- O uso é limitado ao tempo necessário para a circunstância excepcional.
- A justificativa comercial para o uso está documentada.
- O uso é explicitamente aprovado pela gerência.
- A identidade do usuário individual é confirmada antes que o acesso a uma conta seja concedido.

- Cada ação realizada é atribuível a um usuário individual.

n) As credenciais de autenticação nunca devem ser anotadas; o "Intex Bank" incentiva o uso de um gerenciador de senhas, como o OnePassword;

o) Os usuários devem alterar as senhas e entrar em contato com suporte imediatamente se houver qualquer suspeita de que uma senha tenha sido compartilhada ou comprometida;

p) Todas as novas senhas devem ser exclusivas e alteradas na primeira utilização;

q) A autenticação multifatorial é necessária para todo acesso a redes e sistemas de produção que afetam o PCI. Os sistemas MFA devem ser implementados da seguinte forma (8.5.1):

- O sistema MFA não deve ser suscetível a ataques de repetição.
- Os sistemas MFA não podem ser ignorados por nenhum usuário, inclusive usuários administrativos, a menos que especificamente documentado e autorizado pela gerência em caráter de exceção, por um período limitado.
- Pelo menos dois tipos diferentes de fatores de autenticação devem ser usados.
- O sucesso de todos os fatores de autenticação é necessário para que o acesso seja concedido.

r) Credenciais de autenticação diferentes devem ser usadas para acesso a cada ambiente individual do cliente (8.2.3)

s) O MFA é implementado da seguinte forma:

- Em todos os acessos que não sejam de console (remotos) ao CDE;
- Em todos os outros acessos ao CDE ou com impacto na segurança do CDE;
- Não é suscetível a ataques de repetição;
- Não pode ser ignorado por nenhum usuário (administrativo ou não), a menos que seja especificamente documentado e aprovado pela gerência por um período definido;
- Com pelo menos dois tipos de fatores de autenticação;
- Requer uma autenticação bem-sucedida antes de conceder o acesso;

6. Segurança Física

O “Intex Bank” proíbe o armazenamento de quaisquer dados do titular do cartão em mídia física ou removível ou em sistemas de propriedade do “Intex Bank”. Os sistemas que afetam o PCI devem ser hospedados e mantidos usando provedores de serviços em nuvem compatíveis com o PCI. Os requisitos adicionais de segurança física estão descritos na Política de Segurança Física.

a) Todos os dispositivos físicos de POS/POI devem ser inventariados (como marca/modelo e localização do dispositivo) e inspecionados quanto a evidências de adulteração pelo menos **trimestralmente**; os resultados da revisão serão mantidos documentados e armazenados de acordo com a Política de Gestão, Classificação e Proteção da Informação;

b) Todos os funcionários com acesso direto a dispositivos POS/POI devem passar por um treinamento **anual** para garantir que estejam cientes de como identificar e relatar atividades suspeitas e suspeitas de adulteração de dispositivos POS/POI (9.5).

c) Todos os funcionários com acesso direto ao CHD devem passar pelo treinamento **anual** para garantir que estejam cientes de suas responsabilidades de proteger os dados e sistemas do titular do cartão (12.6.3).

d) Os visitantes e fornecedores com acesso ao CDE são acompanhados, claramente identificados e rastreados por meio de processos formalizados de controle de acesso (9.3).

e) As câmeras e o acesso físico à rede são protegidos contra acesso não autorizado, e a entrada/saída do CDE é protegida por meio de cadeados, planilhas de rastreamento, leitores de crachás, câmeras e outros métodos (9.2) (9.3).

7. Registros e Alertas

Além das políticas de registro e alerta estabelecidas na Política de Segurança de Operações e no Plano de Resposta a Incidentes de Segurança, é necessário seguir os seguintes requisitos específicos do PCI:

a) Todo acesso individual aos dados do titular do cartão deve ser capturado em trilhas de auditoria; os registros devem incluir detalhes suficientes para ajudar a determinar ações específicas do usuário no caso de uma investigação (10.2.1);

b) Todos os sistemas críticos devem usar a sincronização de tempo (NTP). Os servidores de tempo devem ser configurados da seguinte forma (10.6):

- As versões do NTP devem ser mantidas atualizadas;

- Os servidores de horário central designados devem ser configurados para receber sinais de horário de fontes externas com base no tempo atômico internacional ou UTC;
- Quando houver mais de um servidor de horário designado, eles devem ser configurados para se comunicarem entre si para manter o horário exato;
- Os sistemas devem ser configurados para receber a hora somente dos servidores de horário central designados;

c) Os eventos dos sistemas críticos do CDE devem ser analisados diariamente pela TI e Cibersegurança e devem usar mecanismos automatizados. A saída de registros detalhados não requer análise diária; eventos anômalos agregados e alertas recebidos de ferramentas automatizadas podem ser analisados para atender a esse requisito. A análise de registros/eventos deve incluir pelo menos o seguinte (10.4):

- Todos os eventos de segurança;
- Registros de todos os componentes do sistema que armazenam, processam ou transmitem CHD e/ou SAD;
- Registros de todos os componentes críticos do sistema;
- Registros de todos os servidores e componentes do sistema que executam funções de segurança, incluindo (firewalls, sistemas de detecção de intrusão/sistemas de prevenção de intrusões (IDS/IPS), servidores de autenticação, servidores de redirecionamento de comércio eletrônico etc.);

A frequência das análises periódicas dos registros em todos os outros componentes do sistema (não definidos no Requisito 10.4.1) deve ser realizada de acordo com todos os elementos especificados no Requisito 12.3.1. Os registros devem ser analisados periodicamente com base na frequência estabelecida pelo “Intex Bank” definida após uma análise de risco direcionada.

O acompanhamento de exceções e eventos anômalos deve ser feito com um chamado. Os eventos críticos de segurança (como suspeita de violação) devem ser encaminhados imediatamente para Cibersegurança para análise e acompanhamento; a Cibersegurança será responsável por determinar se o Plano de Resposta Incidentes de Segurança do “Intex Bank” será acionado.

Todos os registros de eventos críticos devem ser retidos por pelo menos um ano off-line, com pelo menos três meses de registros disponíveis on-line para análise imediata (10.5.1)

As falhas nos sistemas críticos de controle de segurança devem ser detectadas, avisadas e abordadas prontamente. O processo inclui, entre outros, a falha nos seguintes sistemas críticos de controle da segurança:

- Controles de segurança de rede.
- IDS/IPS.
- FIM/Mecanismos de detecção de alterações.
- Soluções antimalware.
- Controles de acesso físico.
- Controles de acesso lógico.
- Mecanismos de registro de auditoria.
- Controles de segmentação (se usados).
- Mecanismos de análise de registros de auditoria.
- Ferramentas de teste de segurança automatizadas (se usadas).

As falhas nos sistemas críticos de controles da segurança devem ser prontamente respondidas, incluindo, entre outros:

- Restaurar as funções de segurança.
- Identificar e documentar a duração (data e hora do início ao fim) da falha de segurança.
- Identificar e documentar as causas da falha e documentar a correção necessária.
- Identificar e resolver problemas de segurança que surjam durante a falha.
- Determinar se há outras ações necessárias após a falha na segurança.
- Implementar controles para evitar que a causa da falha ocorra novamente.
- Retomar o monitoramento dos controles de segurança.

8. Gestão de Vulnerabilidades

a) Os escaneamentos trimestrais de vulnerabilidades internas e externas e os testes de penetração devem ser realizados de acordo com as normas e procedimentos descritos na Política de Segurança de Operações. Os seguintes requisitos específicos da PCI devem ser seguidos:

- Escaneamento interno: os escaneamentos devem ser realizados pelo menos a cada trimestre e após qualquer alteração significativa no ambiente de dados do titular do cartão. Todas as vulnerabilidades de "alto risco" (conforme definido no Requisito 6.3 do PCI DSS) devem ser identificadas, corrigidas ou atenuadas e submetidas a novo escaneamento para validar a resolução do problema. (11.3) Os escaneamentos de vulnerabilidades internas devem ser realizados de forma autenticada da seguinte forma:
  - Os sistemas que não podem aceitar credenciais para escaneamento autenticado

são documentados.

- São usados privilégios suficientes nos sistemas que aceitam credenciais para escaneamento.
- Se as contas usadas para escaneamento autenticado puderem ser usadas para login interativo, elas serão gerenciadas de acordo com o Requisito 8.2.2. (11.3.1.2)

- Todas as outras vulnerabilidades cobertas (as não classificadas como de alto risco ou críticas de acordo com as classificações de risco de vulnerabilidade da entidade definidas no Requisito 6.3.1) devem ser tratadas com base no risco definido via análise de risco direcionada, realizada de acordo com todos os elementos especificados no Requisito 12.3.1. (11.3.1.1)
- Os escaneamentos externos trimestrais devem ser realizados por um prestador de escaneamento externo aprovado e incluir todos os sistemas PCI dentro do escopo. Nos escaneamentos externos, as vulnerabilidades com pontuação CVSS igual ou superior a 4,0 devem ser identificadas, corrigidas ou atenuadas e submetidas a um novo escaneamento para validar a resolução do problema. Deve-se guardar um relatório de escaneamento ASV atestado e aprovado (e evidências de novos escaneamentos) em cada escaneamento trimestral. (11.3)
- A TI deve analisar periodicamente as fontes externas do setor, incluindo feeds de fornecedores e de segurança, para identificar riscos de segurança atuais e contínuos para o “Intex Bank” e distribuir informações que afetem a segurança para as equipes correspondentes via e-mail. Todas as vulnerabilidades identificadas devem ser classificadas como de acordo com a Política de Gestão de Riscos (6.3.1)

b) Para atender a todos os requisitos do PCI DSS, o teste de penetração deve ser realizado por um recurso interno ou externo qualificado, seguindo uma metodologia específica aceita pelo setor, que: (11.4.1)
   - Tenha base em abordagens de teste de penetração aceitas pelo setor (NIST SP800-115 etc.)
   - Cobertura de todo o perímetro do CDE e sistemas críticos.
   - Testes de dentro e de fora da rede.
   - Testes para validar qualquer segmentação e controles na redução do escopo.
   - Teste de penetração na camada de aplicativos para identificar, no mínimo, as vulnerabilidades descritas no Requisito 6.2.4.
   - Testes de penetração na camada de rede que abrangem todos os componentes que aceitam funções de rede e sistemas operacionais.

- Análise e consideração das ameaças e vulnerabilidades vivenciadas nos últimos 12 meses.
- Abordagem documentada para avaliar e tratar o risco representado por vulnerabilidades exploráveis e pontos fracos de segurança encontrados durante os testes de penetração.

c) Retenção dos resultados dos testes de penetração e das atividades de correção por pelo menos 12 meses. Os testes de penetração devem ser realizados anualmente ou em resposta a mudanças significativas no ambiente da PCI. Os testes de segmentação devem ser realizados pelo menos anualmente e após qualquer alteração nos métodos de segmentação (11.4).

d) Todos os resultados de testes de penetração classificados como "exploráveis" (se, por exemplo, podem levar à violação dos sistemas CHD e CDE) devem ser corrigidos ou mitigados e reescaneados para validar a resolução do problema. (11.4.4)

e) Os sistemas de detecção/prevenção de invasão devem estar implementados para monitorar o perímetro e os pontos críticos no ambiente de dados do titular do cartão. Os mecanismos de detecção e prevenção de invasões, as linhas de base e as assinaturas devem ser mantidos atualizados, e os alertas de IDS/IPS devem ser agregados e enviados para a TI como parte das operações diárias de registro e alerta (11.5.1).

f) As técnicas de detecção e/ou prevenção de invasão devem detectar, alertar/prevenir e abordar os canais de comunicação de malware encobertos

9. Manutenção Constante do DSS

9.1. Avaliações de Risco Direcionadas:

Cada requisito do PCI DSS oferece flexibilidade à frequência de sua realização (como, por exemplo, requisitos a serem realizados periodicamente) deve ter respaldo em uma análise de risco direcionada e documentada e que inclua (12.3.1):

- Identificação dos ativos que estão sendo protegidos.
- Identificação das ameaças das quais o requisito está protegendo.
- Identificação dos fatores que contribuem para a probabilidade e/ou o impacto de uma ameaça ser concretizada.
- Análise resultante que determina e inclui justificativa para a frequência com que o requisito deve ser executado para minimizar a probabilidade de a ameaça ser concretizada.
- Revisão de cada análise de risco direcionada pelo menos uma vez a cada 12 meses

para determinar se os resultados ainda são válidos ou se é necessária uma análise de risco atualizada/ML

- Realização de análises atualizadas dos riscos quando necessário, conforme determinado pela revisão anual.

9.2. Hardware e Software:

As tecnologias de hardware e software em uso são revisadas pelo menos uma vez a cada 12 meses e devem incluir pelo menos (12.3.4):

- Análise de que as tecnologias continuam a receber prontamente as correções de segurança dos fornecedores.
- Análise de que as tecnologias continuam a aceitar (e não impedem) o cumprimento do PCI DSS pela entidade.
- Documentação de quaisquer anúncios ou tendências do setor relacionados a uma tecnologia, como quando um fornecedor anunciou planos de "fim de vida" para uma tecnologia
- Documentação de um plano, aprovado pela gerência sênior, para corrigir tecnologias desatualizadas, inclusive aquelas para as quais os fornecedores anunciaram planos de "fim de vida".

9.3. Confirmação do Escopo (12.5.2):

O escopo do PCI DSS deve ser documentado e confirmado pelo menos uma vez a cada 12 meses e mediante alterações significativas no ambiente do escopo.

A validação do escopo deve incluir, no mínimo:

- Identificação de todos os fluxos de dados nos vários estágios de pagamento (autorização, captura, liquidação, estornos, reembolsos etc.) e canais de aceitação (cartão presente, cartão não presente, comércio eletrônico etc.).
- Atualização de todos os diagramas de fluxo de dados de acordo com o requisito 1.2.4.
- Identificação de todos os locais onde os dados da conta são guardados, processados e transmitidos, incluindo, entre outros:

  1) quaisquer locais fora do CDE atualmente definido;

  2) aplicativos que processam CHD;

  3) transmissões entre sistemas e redes; e

  4) backups de arquivos.

- Identificação de todos os componentes do sistema no CDE, conectados ao CDE ou que possam afetar a segurança do CDE.
- Identificação de todos os controles de segmentação em uso e os ambientes dos quais o CDE é segmentado, incluindo a justificativa para ambientes fora do escopo.
- Identificação de todas as ligações de entidades externas com acesso ao CDE.
- Confirmação de que todos os fluxos de dados identificados, dados de contas, componentes do sistema, controles de segmentação e conexões de terceiros com acesso ao CDE estão incluídos no escopo.

9.4. Gestão de Incidentes e CHD (12.10.7):

Os procedimentos de resposta a incidentes devem ser iniciados após a detecção do PAN armazenado em qualquer lugar onde ele não seja esperado; são eles:

- Determinar o que fazer se o PAN for descoberto fora do CDE, incluindo a recuperação, exclusão segura e/ou migração para o CDE atualmente definido, conforme for.
- Identificar se dados de autenticação confidenciais são armazenados com o PAN.
- Determinar a origem dos dados da conta e como eles foram parar onde não eram esperados.
- Corrigir vazamentos de dados ou falhas de processo que resultaram nos dados da conta onde não era esperado.

9.5. Análise Anual do Prestador de Serviços Terceirizado (12.8.X):

Pelo menos uma vez por ano, a TI, juntamente com a equipe de cibersegurança, confirmará os status de conformidade com o PCI DSS de todos os provedores de serviços terceirizados em questão via revisão do AOC em conformidade com o TPSP. Também devem ser mantidas as informações sobre quais requisitos do PCI DSS são gerenciados por cada TPSP, que são gerenciados pelo "Intex Bank" e os que forem compartilhados entre o TPSP e o "Intex Bank".

As avaliações devem ser realizadas pelo menos uma vez a cada três meses para confirmar que o pessoal está realizando as tarefas de acordo com todas as políticas de segurança e procedimentos operacionais. As avaliações serão realizadas por funcionários que não sejam os responsáveis pela execução da tarefa e incluirão, entre outras, as seguintes tarefas.

- Avaliação diária dos registros.
- Avaliação da configuração dos controles de segurança de rede.

- Aplicação dos padrões de configuração a novos sistemas.
- Resposta aos alertas de segurança
- Processos de gestão de mudanças.

Essas avaliações devem ser formalmente documentadas e incluir:

- Os resultados das avaliações.
- Ações de correção, documentadas, tomadas para todas as tarefas consideradas não executadas no Requisito 12.4.2.
- Avaliação e aprovação dos resultados pelo pessoal responsável pelo programa de conformidade com o PCI DSS.

Além disso, o escopo do PCI DSS deve ser documentado e confirmado pelo menos uma vez a cada seis meses e em caso de alterações significativas no ambiente de dados do titular do cartão do prestador de serviços no escopo.

- A validação do escopo deve incluir, no mínimo, todos os elementos especificados acima
- As mudanças significativas na estrutura organizacional devem resultar em uma análise documentada (interna) do impacto no escopo do PCI DSS e na aplicabilidade dos controles, com resultados comunicados à gerência executiva.

10. Exceções

Exceções a esta política devem ser formalmente submetidas ao Gestor de Tecnologia da Informação e ao Encarregado de Proteção de Dados (DPO) para avaliação e aprovação, garantindo que cada caso seja devidamente documentado e justificado.

Em casos de dúvidas, comentários ou necessidade de exceções, entre em contato pelo e-mail ciberseguranca@trevisocc.com.br

11. Violações e Não Cumprimentos da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Gestor de Tecnologia da Informação e ao Encarregado de Proteção de Dados para as providências cabíveis. Violações poderão resultar em sanções administrativas, incluindo a perda de privilégios de acesso a sistemas e redes, bem como medidas disciplinares conforme os procedimentos internos do “Intex Bank”, que podem incluir rescisão de contratos ou parcerias.

12. Vigência

Esta política entra em vigor na data de sua publicação, sendo revisada no prazo de 18 (dezoito) meses, ou a qualquer momento, conforme a necessidade.

São Paulo, 05 de junho de 2025.

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 05/06/2025.

Apêndice A: Padrões de Configuração do PCI

1. Padrões de Rede

a) O gerenciamento das regras e das configurações de rede só pode ser realizado por membros autorizados da equipe de TI, e todas as alterações e devem cumprir os procedimentos de gerenciamento de mudanças definidos na Política de Segurança de Operações (1.2.2).

b) Devem-se criar e sempre atualizar os diagramas de fluxo de dados da rede e do titular do cartão. Alterações significativas (adição ou eliminação de VPCs e sub-redes, novas conexões externas etc.) devem ser documentadas nos diagramas; mesmo que nenhuma alteração tenha ocorrido, os diagramas devem ser revisados pelo menos anualmente para fins de precisão; e aprovados (no campo do número da versão/data etc.) por membros autorizados da equipe de TI (1.2.3) (1.2.4). As configurações dos controles de segurança da rede devem ser revisadas pelo menos uma vez a cada seis meses para confirmar que são relevantes e eficazes. Os resultados da revisão devem ser documentados e armazenados de maneira segura.

c) Os controles de rede aceitos nas redes de produção são firewalls, roteadores com listas de controle de acesso (ACLs), dispositivos virtuais, controles de acesso à nuvem e tecnologias de rede definidas por software (SDN). A gestão dos sistemas de rede de produção é feita via sistemas de gerenciamento remoto como SSH (Secure Shell), interfaces web seguras e ferramentas de gerenciamento fora de banda (ex: IPMI, KVM-over-IP), desde que protegidas com criptografia forte. Toda a gestão dos sistemas PCI exige o uso de autenticação multifatorial e o uso de criptografia forte. (2.2.7).

d) No ambiente de produção, devem-se seguir as regras e configurações definidas para controlar o tráfego das redes não confiáveis (serviços disponíveis ao público etc.) para redes internas (sistemas de gestão etc.);

e) Todos os serviços, protocolos e portas permitidos dentro e fora do CDE devem ser identificados, aprovados e ter uma demanda de negócios definida, além de ser devidamente documentada (1.2.5).

f) Não são permitidas conexões diretas entre as ZONAS INTERNAS e a Internet; e todo o tráfego de e para a ZONA INTERNA deve ser limitado a endereços na DMZ ou equivalente. As exceções devem ser documentadas e aprovadas, e devem-se implementar e testar controles de segurança suficientes (1.4).

g) Devem-se configurar os sistemas de controle de rede para usar a tradução de

endereços de rede padrão, a fim de evitar a divulgação de endereços IP internos na Internet. Se forem usados endereços IP privados, qualquer divulgação a terceiros deverá ser devidamente autorizada, documentada e revisada periodicamente quanto às demandas de negócios (1.4.5).

h) Os aparelhos móveis que se conectam às redes de produção devem usar firewall pessoal ou equivalente (como proteção de endpoint com restrições de rede ativadas). É proibido desativar ou ignorar os firewalls pessoais enquanto estiver conectada aos sistemas do "Intex Bank" (1.5.1).

i) Todos os sistemas de controle de rede devem ser configurados com regras padrão antispoofing para bloquear ou negar endereços internos de entrada ou endereços IP falsos com origem na Internet (1.4.3).

j) Os sistemas de controle de rede só podem permitir conexões estabelecidas na rede interna e devem negar quaisquer conexões de entrada não associadas a uma sessão já estabelecida (1.4.2).

k) Todo o tráfego de redes não confiáveis para os sistemas internos deve ser autorizado e limitado a serviços, protocolos e portas definidos, com acesso ao público com configurações stateful. Todos os outros tráfegos não explicitamente permitidos devem ser bloqueados ou eliminados. (1.4.2).

l) São proibidos os intervalos de portas e IP, a menos que sejam especificamente examinados e justificados; todos os serviços disponíveis devem ser documentados e justificados e devem aceitar configurações seguras; todas as outras portas, serviços e tráfego de rede devem ser especificamente negados (1.2) (1.3) (2.2).

m) É proibido o uso de serviços e protocolos inseguros sem justificativa e documentação complementar dos recursos de segurança implementados para reduzir riscos (1.2.6) (1.3) (2.2) (2.3).

n) As sessões de acesso remoto devem ser configuradas para se encerrarem após um período especificado de 8 horas (12.2.1).

o) As tecnologias de acesso remoto para prestadores e parceiros de negócios usadas para acessar sistemas de produção devem ser ativadas somente quando necessário para fins de negócios e desativadas imediatamente após o uso (8) (12.2.1).

p) NACLs, portas, zonas e serviços específicos permitidos dentro e fora do ambiente de produção da PCI estão definidos abaixo: as regras e o tráfego permitido devem ser avaliados pelo menos a cada seis meses e formalmente aprovados pela equipe de TI, juntamente com a equipe de cibersegurança (1.3) (1.4):

2. Configurações de Nível de Sistema do PCI

Todos os sistemas que impactam o PCI devem cumprir os seguintes requisitos técnicos:

a) Todos os padrões do prestador (incluindo senhas padrão nos sistemas operacionais, software que presta serviços de segurança, contas de aplicativos e sistemas, terminais POS, cadeias de caracteres comunitárias do Simple Network Management Protocol (SNMP) etc.) devem ser alterados antes que um sistema seja instalado na rede (2.2);

b) As contas padrão desnecessárias (incluindo contas usadas pelos sistemas operacionais, software de segurança, aplicativos, sistemas, terminais POS, SNMP etc.) devem ser excluídas ou desativadas antes que um sistema seja instalado na rede (2.2);

c) Apenas uma função principal pode ser implementada por servidor para impedir que funções que exigem diferentes níveis de segurança coexistam no mesmo sistema (2.2);

d) Somente os serviços, protocolos, daemons, etc. necessários podem ser ativados, e somente conforme necessário para o funcionamento do sistema. Todas as funcionalidades desnecessárias (como scripts, drivers, recursos, subsistemas, sistemas de arquivos e servidores web) devem ser desativadas (2.2);

e) No Apêndice A deste documento, devem-se documentar os recursos complementares de segurança para quaisquer serviços, protocolos ou daemons necessários que sejam considerados inseguros. Deve-se justificar e testar para garantir que não tragam riscos nem vulnerabilidades desnecessárias (1.2.6, 2.2);

f) Todos os patches de segurança identificados como médio ou alto devem ser aplicados aos sistemas dentro 60 dias de acordo com a Política de Segurança de Operações; os patches de segurança críticos devem ser aplicados dentro de 30 dias.

3. Padrões Sem Fio

Os pontos de acesso sem fio usados no ambiente de produção devem obedecer às seguintes configurações do sistema (2.3):

a) As cadeias de comunidade SNMP padrão precisam ser alteradas na instalação;

b) As senhas/frases padrões nos pontos de acesso devem ser alteradas na instalação; as senhas/frases secretas devem ser alteradas sempre que o pessoal com conhecimento da chave deixar a empresa ou a função para a qual o conhecimento era necessário; ou

c) Sempre que houver suspeita ou conhecimento de que uma chave foi violada (2.3.1);
d) O firmware e as configurações dos aparelhos sem fio conectados ao ambiente de produção devem ser atualizados periodicamente para que os pontos de acesso:
    - Aceitem criptografia forte nas funções de gestão e transmissão dos dados nas redes sem fio
    - Exigem a autenticação nas redes sem fio (redes sem convidados).
    - As configurações relacionadas à segurança (como páginas e contas de administração padrão) devem ser alteradas ou atualizadas para aceitarem configurações seguras.
    - Deve-se ter um firewall ou sistema de controle de acesso equivalente instalado entre qualquer rede sem fio e o ambiente de produção (1.3.3).

Apêndice B: Serviços e Portas Inseguras

É proibido o uso de serviços e protocolos inseguros sem justificativa e documentação complementar dos recursos de segurança implementados para reduzir riscos. Os serviços a seguir foram identificados (por meios manuais ou técnicos) como "inseguros" (normalmente devido à maior probabilidade de abuso do serviço ou ao uso de um protocolo fraco ou não criptografado). Todos os protocolos inseguros usados para aceitar zonas e serviços de produção exigem complementação na análise de risco, na justificativa de negócios e na documentação de recursos de segurança implementados, a fim de eliminar ou atenuar os riscos introduzidos:

Serviço	Porta	Impacto/descrição	Justificativa de negócios	Controles de segurança implementados
FTP	tcp/21	O FTP não seguro pode permitir o acesso não autorizado ou a interceptação de dados confidenciais e informações de autenticação	O FTP é exigido por vários parceiros como o único protocolo aceito na transferência de arquivos em lote	▪ Exige lista branca de IPs ▪ Não são permitidos logins genéricos ▪ P2P (linhas privadas/alugadas) usadas por cliente ▪ Todos os dados são criptografados com chaves GPG fortes ▪ Eliminação automatizada dos dados após o processamento do arquivo dentro de 24 horas ▪ Serviço FTP monitorado 24 horas por dia via SIEM/Cloudwatch
HTTP	tcp/80	O HTTP não seguro pode permitir o acesso não autorizado ou a interceptação de dados	O HTTP é aceito no site de RP voltado para o público. Nenhum	Nenhum CHD foi enviado por HTTP.

		confidenciais e informações de autenticação	CHD é processado nem transmitido via HTTP.	
Serviço 3				
Serviço 4				

Apêndice C: Processo de Aviso sobre a Violação da Bandeira do Cartão

Esta seção traz informações específicas sobre as violações na segurança relacionadas ao CHD; os requisitos mínimos à bandeira de cartão de crédito; e os detalhes sobre quem envolver para garantir a conformidade. Confira a seguir os passos em caso de violação ou suspeita de violação que envolva a perda ou o acesso não autorizado aos Dados do Titular do Cartão:

1. O Gerente de TI entrará em contato com o Jurídico, que entrará em contato com Relações Públicas e os órgãos responsáveis. Se for um incidente passível de denúncia, esse grupo será responsável por denunciá-lo à polícia e solicitar uma investigação e perícia externas. Cada bandeira mencionada posteriormente nesta seção também pode orientar sobre as próximas etapas, como a necessidade de procurar um perito em PCI (PFI). Devem-se tomar todas as medidas necessárias para conter novas violações nos registros (desativar o acesso externo etc.), mas, sempre que possível, os sistemas afetados devem ser mantidos em funcionamento para facilitar uma potencial perícia.

a. O Gerente de TI será responsável por incluir os recursos técnicos do "Intex Bank" para coletar, no mínimo, as seguintes informações:

- Número de contas em risco, identificando aquelas guardadas e violadas
- Tipo de informações da conta em risco
- Números de contas
- Datas de vencimento
- Nomes dos titulares do cartão
- Endereços dos titulares do cartão
- Se algum dado foi exportado e para onde.
- Como ocorreu a violação
- A origem da violação
- O período da violação
- Se a violação foi contida

b. O departamento de Relações Públicas será responsável por elaborar uma declaração de aviso, a ser emitida para as pessoas afetadas pela perda dos dados. O aviso deve ser emitido no momento adequado, ficar bem visível e ser entregue de forma a garantir que o indivíduo a receba. Os métodos apropriados de entrega são:

- Aviso alternativo ao e-mail e aos correios (apenas para quem não pode ser contatada por correio nem e-mail);

- Publicação visível do aviso na página inicial do “Intex Bank”;
- Aviso nos principais meios de comunicação;
- O aviso deve incluir:

1 Uma descrição geral do incidente;

2 Medidas que as pessoas podem tomar para mitigar os danos, incluindo o monitoramento dos relatórios de crédito e alertas de fraude, bem como fontes de informações voltadas para o público se proteger do roubo de identidade;

3 Um lembrete para continuar vigilante nos 12 a 24 meses seguintes; e

4 O número ou canal de comunicação do atendimento ao cliente para o qual as pessoas podem ligar.

Procedimentos específicos de resposta à violação dos dados do titular do cartão

A seguir, detalhamos os contatos da bandeira do cartão e os procedimentos de resposta esperados de todos os comerciantes e prestadores de serviços caso os dados do titular do cartão tenham sido violados.

1. VISA

Toda entidade que suspeite ou confirme o acesso não autorizado a qualquer dado do titular do cartão Visa, incluindo entidades que guardam, processam ou transmitem dados do titular do cartão ou que tenham acesso a um ambiente ou sistemas de pagamentos, é obrigada a aderir aos requisitos do WTDIC. Isso inclui, entre outras, todas as instituições financeiras membros da Visa (Emissores, Adquirentes), Comerciantes, Processadores, Gateways, Agentes, Prestadores de Serviços, Fornecedores Terceirizados, Revendedores Integradores e quaisquer outras entidades, bem como outros participantes do sistema de pagamento que operam ou acessam um ambiente de pagamentos.

A entidade violada deve enviar um aviso à Visa dentro de três (3) dias corridos, seguindo as diretrizes documentadas em:

https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

2.MasterCard

Exceto na medida em que for proibido pela lei ou regulamentação aplicável, cada Cliente PTA deverá notificar a Empresa (inclusive por e-mail para: **account_data_compromise@mastercard.com** e para qualquer Incidente de Segurança

relacionado a Dados Pessoais, por telefone, para o Centro de Comando de Operações (OCC) da Empresa, no endereço: **1-636-722-6220 ou 1-800-358-3060,** selecionando a opção para o Centro de Operações de Segurança da Empresa imediatamente após a identificação de que algum Titular da Conta, indivíduo ou entidade violou ou potencialmente violou as medidas de segurança do Cliente PTA ou obteve acesso não autorizado a quaisquer Dados Pessoais mantidos pelo Cliente PTA, e, em particular, de qualquer incidente ou violação na segurança que resulte na destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos Dados Pessoais transmitidos, guardados ou processados de outra forma pelo Cliente PTA, e que esteja ciente de qualquer incidente ou possível incidente em Transações PTA fraudulentas (qualquer um dos itens acima, "Incidente de Segurança"). O aviso deve incluir todas as informações e comprovações necessárias para satisfazer a Corporação.

Após a descoberta desse tipo e entre outras ações, o Cliente PTA deverá investigar, remediar e atenuar imediatamente os efeitos do Incidente de Segurança e repassar à Corporação informações que garantam razoavelmente à Corporação que esse Incidente de Segurança não ocorrerá novamente.

https://www.mastercard.us/content/dam/mccom/global/documents/mastercard-rules.pdf

3.Discover

Para comunicar uma violação dos dados:

Ligue para 1-800-347-3083

4.American Express

Você deve avisar imediatamente o American Express e, em até 24 (vinte e quatro) horas após a descoberta de um Incidente de Dados.

Para avisar o American Express, procure a equipe EIRP da American Express em:

+1 (888) 732-3750 (ligação gratuita nos EUA) ou +1 (602) 537-3021 (internacional)

-ou-

envie um e-mail para EIRP@aexp.com. Preencha o formulário Incidente com os dados do comerciante - Formulário de aviso inicial e anexe-o ao e-mail.

https://www.americanexpress.com/content/dam/amex/us/merchant/merchant-channel/Data_Incident_What_do_I_do_Final_US.pdf

Em caso de incidentes de dados, deve-se contatar o DPO por meio do endereço: dpo@trevisocc.com.br.