Certificação de Segurança para Dispositivos de Captura de Senhas

Comitê Segurança e Prevenção a Fraude

Ano 2016
Versão 7.0

Av. Brigadeiro Faria Lima, 1485 | 13º andar | Torre Norte
Jardim Paulistano | São Paulo (SP) | CEP 01452 921
(11) 3296 2750 l abecs@abecs.org.br
www.abecs.org.br

INDICE

Histórico de revisões

Revisão	Data	Descrição
Manual_ABECS_v4	13/07/2009	Versão inicial
Manual_ABECS_v5	13/07/2010	Item: 1.4.1 Visão Geral - Atualização de conteúdo. Item: 4. Processos de homologação - Alteração dos fluxos. Item: 4.1. Definição - Atualização de conteúdo. Item: Processo utilizado pelas credenciadoras – Exclusão deste item. Item: 4.5. Periodicidade de revisões – Inclusão deste item Item: 5. Pré-requisito para Certificação – Inclusão deste item Item: 6. Recertificação – Inclusão deste item Item: 7.1.1 Requisitos ABECS 01 – Inclusão do requisito b). Item: 5.1.2 Requisitos ABECS 02 - Atualização de conteúdo. Item: 7.1.3 Requisitos ABECS 03 – Inclusão do requisito b). Inclusão do 7.1.7 Requisitos ABECS 07 Item: 9. Referencias externa (PCI-PTS) – Inclusão de tabela de referencias. Item: 10. Terminais homologados pelo Comitê ABECS. – Atualização titulo e tabela.
Manual_ABECS_v6	13/07/2012	Item: 3. Escopo – Inclusão do PCI-PTS 3.x. Item: 4.4.2 Auditorias - Atualização de conteúdo. Item: 7.1.2 Requisitos ABECS 02 - Atualização de conteúdo. Item: 9. Laboratórios Homologados - Atualização de conteúdo. Item: 11. Terminais homologados pelo Comitê ABECS. – Inclusão de novos terminas certificados.
Manual_ABECS_v7	25/07/2016	Excluído o Item 6 (Recertificação)sendo acrescentado ao item 5. Renumerado os itens. Antigo 7.1.1; novo 6.1.1 Requisitos ABECS 01(Melhoria) Antigo 7.1.3; novo 6.1.3 Requisitos ABECS 03(Inclusão de item) Antigo 7.1.4; novo 6.1.4 Requisitos ABECS 04(Inclusão de item) Antigo 7.1.7; novo 6.1.7 Requisitos ABECS 07(Melhoria/Inclusão) 11.1 Retirada a lista de Terminais homologados pelo Comitê ABECS.

1. Introdução

1.1. Motivação

O crescente número de cartões emitidos pelos bancos e consequentemente, o aumento do número de transações eletrônicas realizadas para pagamentos de bens e serviços em estabelecimentos comerciais torna a clonagem de cartões um ato rentável, pois os dados do portador podem ser utilizados tanto no Brasil como no exterior.

Existem diversas técnicas de cópia de trilhas e senhas para posterior clonagem. Uma delas é a inserção de um dispositivo aos equipamentos de captura POS (point-of-sale) e PINPAD (Personal identification number Pad). Nas avaliações efetuadas pelas credenciadoras, nota-se um claro avanço tecnológico desta técnica no Brasil comparada com os outros países que aceitam cartões de crédito e débito.

1.2. Benefícios para o mercado

O PCI SSC permitirá que os fornecedores de PED's desenvolvam de uma forma mais fácil, rápida e rentável o processo de avaliação de segurança. Com isso poderão reduzir a complexidade de um novo produto em desenvolvimento em um único processo de avaliação e proporcionar uma colocação do mercado para as instituições e credenciadoras.
No passado, os fornecedores de PED's tinham de passar por vários testes diferentes para atender os requisitos de segurança de todo o regime de meios de pagamentos globais e locais. Isto se tornou caro, e muitas vezes criou confusão nos critérios que eram avaliados. Por este motivo foi definido que a ABECS ficará responsável pela validação de todos os testes de segurança e validação de requisitos mínimos, seguindo as regras do PCI SSC.
Reunimos normas e regras para avaliação dos fornecedores de forma que todos serão beneficiados pela redução de custo e tempo e complexidade das operações de meios de pagamentos.

1.3. PCI SSC

Em setembro de 2006, as principais bandeiras de cartões de crédito e débito (Amex, Discover Financial Services, JCB, MasterCard Worldwide e Visa International) criaram um conselho chamado PCI Council que também é composto por diversas empresas, o mesmo foi designado a criar e recomendar melhores práticas de segurança de dados, a serem seguidas pelos estabelecimentos comerciais e processadoras que aceitam cartões como forma de pagamento, o principal motivo é proteger a privacidade dos consumidores portadores de cartões.

Dentre as diversas ações geradas pelo PCI SSC a mais relevante foi o alinhamento entre as bandeiras que incorpora:

- Fundamentação Técnica: Requisitos para armazenamento, processamento e transmissão segura de dados do portador.

- Metodologias de Testes: Procedimentos comuns de auditoria, testes de vulnerabilidades e questionário de auto-avaliação.

O PCI SSC se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão. Em linhas gerais, esta adaptação inclui comerciantes, intermediários que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, assim como provedores de serviço que hospedam sites, processam transações em ATM ou coletam e processam dados de cartão de crédito em nome de membros das redes Visa e Mastercard - gateways de pagamento, também se aplica aos fabricantes, que especificam e implementam dispositivo de característica de gestão numérica de identificação pessoal (PIN) entrada de terminais, PCI-PTS.

1.4. PCI PTS (Payment Card Industry PIN Transaction Security)

1.4.1 Visão Geral

No passado, o PED Security Requirements era supervisionada pelo JCB, MasterCard e VISA. Agora, através do PCI SSC, as cinco principais marcas mundiais de meios de pagamento (American Express, Discover, JCB, MasterCard e Visa) irão gerir as exigências de segurança do programa PTS, permitindo padronizar os requisitos dos dispositivos de segurança, metodologia de testes e processos de aprovação para PIN Transaction Security (PTS).
É prioridade estratégica para o PCI SSC continuar a racionalizar as normas de segurança e garantir o desenvolvimento de dispositivos. Tornando mais consistentes as medidas de segurança com custos eficazes para sua implantação no mercado.

O PCI-PTS Security Requirements se preocupa com os dispositivos e características técnicas que impactam a segurança do PIN.

O PIN (Personal Identification Number) é utilizado pelo titular do cartão durante uma operação financeira.

As características físicas dos dispositivos devem considerar sensores de segurança para identificar e tratar ataques físicos aos equipamentos, como por exemplo: Abertura do terminal, instalação de dispositivos fraudulentos, etc.

O lógico são características de segurança que incluem as capacidades funcionais que impeçam o acesso a dados dos terminais, como por exemplo, copia da aplicação, acesso a chaves criptográficas e dados processados.

A gestão do PED é rigorosa, a fim de que seja produzido e controlado de maneira que seja incapaz de transportar um skimmer (conhecido como chupa cabra), ou de comprometer o processo de criptografia. Se o dispositivo não for adequadamente controlado podem ocorrer modificações não autorizadas as suas características físicas e lógicas de segurança.

2. Objetivo ABECS

Definição de Requisitos mínimos de segurança para os dispositivos de captura de transações eletrônicas no Brasil, critérios de avaliação e processos para realização destas avaliações.

A ABECS reuniu normas e regras para avaliação dos fornecedores de forma que todos serão beneficiados pela redução de custo e tempo e complexidade das operações de meios de pagamentos.

3. Escopo

Equipamentos de captura de senha (POS e PIN PAD) homologados pelo PCI PTS nas versões 3.x ou superior.

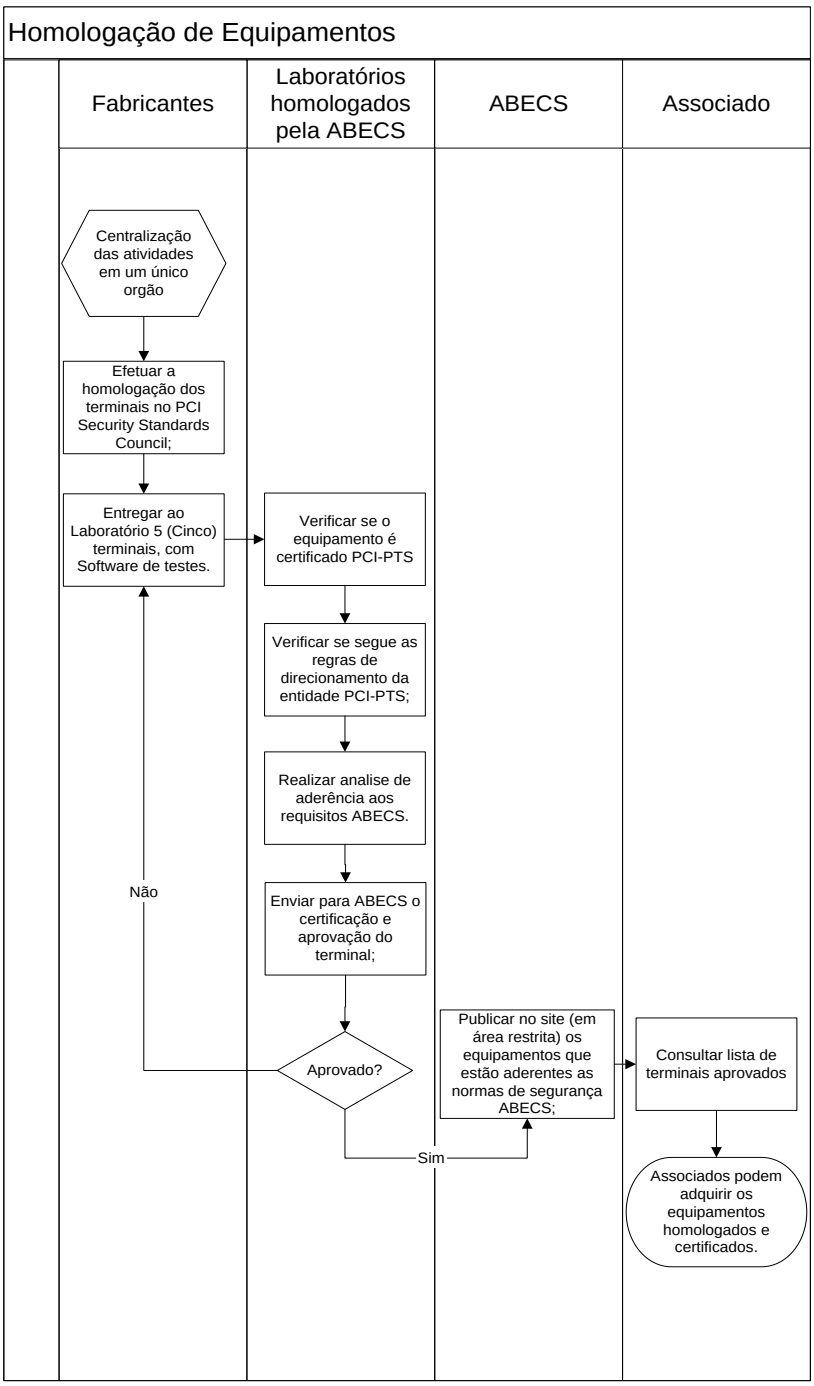
4. Processos de homologação

4.1. Definição

Estes processos contemplam os Requisitos para os equipamentos, critérios de testes destes equipamentos, critérios de homologação de laboratórios e controle de qualidade dos testes efetuados.

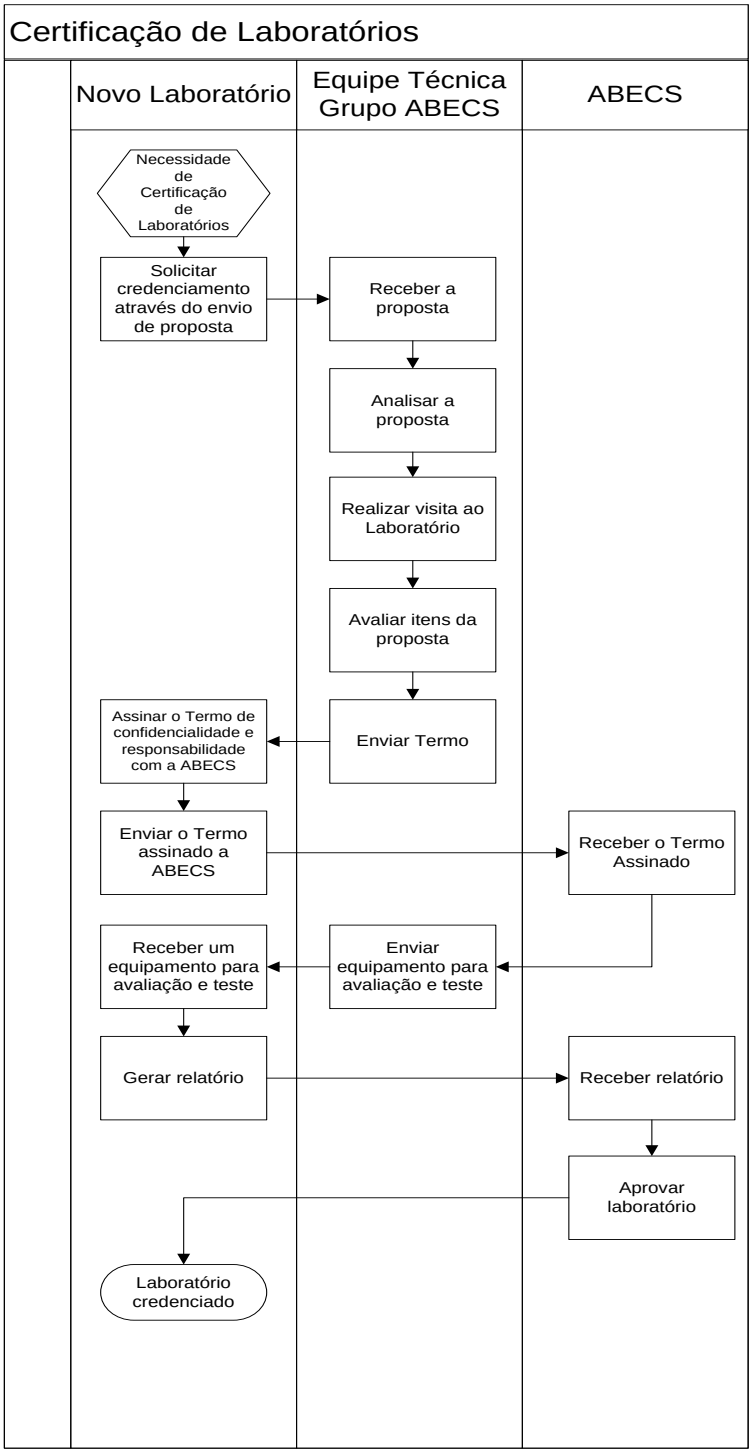
4.2. Fluxo de homologação de equipamentos

O fluxo de homologação dos equipamentos tem como principal objetivo centralizar as validações técnicas e lógicas dos fabricantes de PED's em um único órgão.



4.3. Fluxo de certificação de laboratórios

Laboratório solicita à ABECS o seu credenciamento através do envio de proposta contendo a descrição de sua experiência, trabalhos já executados nesta área ou em áreas similares, instalações e perfil dos técnicos que atuam para a empresa.



4.4. Controle de qualidade e confidencialidade

4.4.1 Termo de confidencialidade e qualidade de serviços

Cada Laboratório homologado pela ABECS deverá firmar com esta entidade um termo de confidencialidade e qualidade (anexo a este documento) com a finalidade de garantir a confidencialidade das informações e também que o mesmo irá seguir todos os procedimentos de testes estipulados pela ABECS.

4.4.2 Auditorias

Caberá á equipe técnica da ABECS responsável pelo PCI à auditoria periódica nos laboratórios para análise da qualidade dos serviços prestados. Esta auditoria deverá ser previamente agendada, porém não haverá um calendário fixo. A equipe técnica da ABECS é composta pelos responsáveis de cada Adquirente, que em conjunto deveram auditar os processos nos Laboratórios, listados no item 9 deste documento.

4.4.3 Periodicidade de revisões

A revisão do processo de homologação de terminais e também de toda documentação gerada para suportar o processo, está divida em três cenários:

Revisão anual: Acontecera sempre no mês de Julho de cada ano e terá como finalidade promover atualização de conteúdo.

Revisão dos Requisitos: Acontecera a cada dois anos e terá a finalidade de incluir, alterar ou excluir Requisitos.

Revisão emergencial: Acontecera sempre que for encontrada uma nova vulnerabilidade nos terminais e seja necessário incluir um novo requisito, para testar essa vulnerabilidade em novos terminais.

5. Pré-requisito para Certificação/Recertificação

5.1. Fabricantes: Neste momento o fabricante poderá certificar a família de terminais ou apenas um modelo. É necessário preparar cinco terminais de cada modelo, com aplicativo que gerencie os sensores de segurança do terminal e seja capaz de bloqueá-lo em situações de ataque físico, realizado pelo laboratório.

5.2. Recomendação ABECS: As recomendações são avaliadas, porém o não atendimento não afeta a certificação. Porém, os resultados da avaliação dos itens de recomendação devem constar do relatório detalhado.

5.3. Laboratórios: Receber os terminais e realizar os testes dentro do prazo estipulado. A tabela abaixo representa as horas destinadas a analise de um modelo de terminal.

Nome da tarefa	Duração	Hora Analista
Analise internas do terminal (Medições Circuitos, componentes e montagem)	12hrs	Hora Analista
Preparação da documentação	20hrs	Hora Analista
Realização de ataque ao terminal	48hrs	Hora Analista
Total	80hrs	Hora Analista

6. Requisitos

6.1. Equipamentos

6.1.1 Requisitos ABECS 01

Tipo:
Físico

Data de início de validade:
Imediata

Descrição:
Deverá existir uma proteção física que impeça a neutralização da segurança do terminal, através do acesso aos sensores de segurança por orifícios existentes ou criados na carcaça. Esta implementação deverá ser feita de tal sorte que não seja possível neutralizar a segurança do terminal independente da quantidade de sensores que foram protegidos, isto é, mesmo neutralizando alguns sensores, a segurança do terminal não poderá ser neutralizada.
Os sensores de segurança por pressão deverão ser protegidos por outro sistema / mecanismo de segurança.
Recomendação ABECS[1]: Mesh de proteção (também conhecido com manta de proteção, muito utilizado no circuito de proteção dos teclados dos equipamentos).
Obrigatoriamente toda mesh deverá ter no mínimo dois layers.

Critério de avaliação:

Neste item, os laboratórios considerarão apto o equipamento quando:
1. Não for possível quebrar esta barreira no prazo estabelecido no item 5.3 para nova certificação ou para recertificação, usando equipamentos convencionais (chave de fenda, alicate, multímetro, osciloscópio, etc.) e sem o conhecimento prévio dos circuitos ou uso de equipamentos mais sofisticados como, por exemplo, Raios-X.
2. Usando no máximo 5 equipamentos por modelo.
3. **Avaliar os sistemas de segurança e os meios de proteção adicionais aos circuitos de pressão de segurança.**
4. **Avaliar a quantidade de layers das mesh aplicadas nos circuitos de segurança quando utilizado mesh.**

6.1.2 Requisitos ABECS 02

Tipo:
Físico.

Data de início de validade:
Imediata

Descrição:

O PinPad deve prover um mecanismo de proteção na conexão com seu cabo de comunicação, de forma que fique visível ao lojista qualquer tentativa de substituição e que dificulte a substituição deste dispositivo de forma rápida ou indevida.

PinPad que permite a retirada do seu conector/cabo deve apresentar mecanismo de fixação, do conector/cabo ao PinPad.

Critério de avaliação:

1. Neste item, os laboratórios considerarão apto o equipamento se para sua substituição for necessário o uso de ferramentas especiais (exemplo chave de fenda) ou rompimento de lacre (cuja ação exija esforço e tempo para execução).

6.1.3 Requisitos ABECS 03

Tipo:
Físico e Lógico

Data de início de validade:
Imediata

Descrição:

O fabricante deve manter a unicidade dos números de série dos dispositivos por ele fabricados de modo a garantir uma identidade única para cada dispositivo de captura.

Não há impeditivos para que um fabricante insira um número já existente em uma nova placa devido à necessidade de substituição de uma placa defeituosa.

Critério de avaliação:

1. Os laboratórios devem solicitar do fabricante a lógica de geração do número de série e acrescentar esta informação ao seu laudo e **ao Relatório Executivo.**
2. O numero de serie interno gravado na memória do terminal deve ser idêntico ao numero gravado na etiqueta externa.
3. Quando ligado o terminal deverá apresentar o número de série interno do equipamento registrado no firmware (quando possuir display). Ou no processo de boot ao apertar a tecla limpa <amarela>, o número de série deverá ser apresentado por 5 segundos, e após este tempo o processo de boot deverá prosseguir normalmente.

6.1.4 Requisitos ABECS 04

Tipo:
Lógico

Data de início de validade:
Imediata

Descrição:

Em caso de tentativa de violação, o dispositivo de captura deverá ativar o mecanismo de resposta à violação que compreende em:

- Remover chaves de criptografia;
- Remover dados de configuração;
- Remover todos os softwares instalados com exceção ao Sistema Operacional;
- Terminal deve ficar “inoperante” não sendo possível que o aplicativo funcione sem a intervenção de um laboratório autorizado.
- Recomendação ABECS²: Que quando em TAMPER o terminal deverá mostrar o número de série do equipamento registrado no firmware além da mensagem de TAMPER.

Critério de avaliação:

1. Os laboratórios devem verificar se o terminal perdeu as chaves de criptografia e também os aplicativos sendo que os mesmos não devem funcionar somente com uma carga do aplicativo pin a pin.

6.1.5 Requisitos ABECS 05

Tipo:
Lógico

Data de início de validade:
Imediata

Descrição:

Todo software carregado no dispositivo de captura deverão ser assinados digitalmente pelo fabricante do dispositivo com a possibilidade de também serem assinados digitalmente pelo fabricante do software e pelo adquirente.

Critério de avaliação:

Os laboratórios deverão avaliar:
1. Se há como colocar uma aplicação não assinada em terminal com assinatura digital.
2. Se há como colocar uma aplicação assinada com um certificado diferente do injetado pelo fabricante.

Os fabricantes deverão entregar os meios necessários para os testes.

6.1.6 Requisitos ABECS 06

Tipo:
Lógico

Data de início de validade:
Imediata

Descrição:

Nos dispositivos de captura em produção não deverá ser possível:

- A desativação de funcionalidades de segurança;
- A impressão ou visualização no display da trilha completa de cartões;
- A visualização da chave de criptografia;
- A inserção manual de chaves de criptografia;

Critério de avaliação:

Os laboratórios devem verificar se existem condições de execução das ações acima. Devem contar com a colaboração do fabricante.

6.1.7 Requisitos ABECS 07

Tipo:
Físico

Data de início de validade:
Imediata para dispositivos de captura que possuam a versão **PCI-PTS 3.x** ou superior.

Descrição:
Não deverá ser possível o acesso à leitora de cartão magnético do terminal, através de orifícios existentes ou criados na carcaça sem que fique evidenciado ou por alterações visíveis no gabinete do terminal ou pelo acionamento do mecanismo de segurança.

Deverão estar protegidos:

1. **Conectores da cabeça magnética tanto na cabeça bem como no conector da cabeça magnética na placa do equipamento;**
2. **Conectores da leitora de CHIP;**
3. **Potenciais meios eletrônicos, como: resistores, transistores, pontos de testes de placas por onde possa passar os dados do portador do cartão antes que os dados cheguem ao processador criptográfico.**

Critério de avaliação:
Caso o laboratório consiga acessar a área onde está instalada a leitora de cartão magnético, sem alterações visíveis no gabinete ou bloqueio do terminal, é necessário evidenciar a captura de dados a partir deste ponto.

A evidência deve ser colhida da seguinte forma:

a) Instalação de dispositivo paralelo das leitoras de cartão ou em seus conectores.

b) Instalação de dispositivos em pontos na placa que possam capturar dados do portador do cartão

c) Deverá demonstrar o log da informação capturada pelo dispositivo paralelo.

d) Demonstrar se a informação está legível ou criptografada.

Observação: Para a leitora de chip, não será considerado válido testes de inserção pelo bocal do leitor, simulando um cartão.

7. Relatórios gerados pelos laboratórios

Quando o terminal for reprovado o relatório gerado deve ser enviado apenas ao fabricante. Para terminais aprovados será necessário enviar os relatórios da seguinte forma:

A – Relatório detalhado: Envio apenas ao fabricante do terminal.
B – Relatório simplificado: Envio apenas a ABECS.

Importante:

- O relato simplificado evita divulgação “pública” dos ataques aos terminais.
- Os relatórios devem ser enviados de forma segura, como por exemplo, criptografados.

O laboratório deverá criar um check-list onde as informações do tipo opcionais estão ou não presentes no equipamento podendo também ter um sistema de notas para cada um dos itens da especificação, tal check-list deverá ser enviado a ABECS e a ABECS enviará aos Adquirentes membros.

8. Laboratórios Homologados

Instituto de Pesquisas Eldorado, localizado na cidade de Campinas, Estado de São Paulo, na Avenida Alan Turing, 275, Campus Unicamp, Cidade Universitário, CEP 13083-898 – Contato Comercial: Sr. Leandro Soares negocios@eldorado.org.br (19) 3757-3202 – Contato Técnico: Rodolfo Lazaretti – rodolfo.lazaretti@eldorado.org.br – (19) 3757 -3507.

Fundação CPqD Centro de Pesquisa e Desenvolvimento em Telecomunicações, com sede na Rua Dr. Ricardo Benetton Martins, 1.000 – Parque II do Polo de Alta Tecnologia - CEP 13086-510 (CEP exclusivo 13086-902), na cidade de Campinas, estado de São Paulo, inscrita no CNPJ sob o nº 02.641.663/0001-10 - Contato Comercial: Mattos, Eduardo M - mattos@cpqd.com.br - (11) 99655-8236 | Contato Técnico: Gustavo Sinzato - gsinzato@cpqd.com.br – (19) 99194-2635 | Ricardo Chibim - rchibim@cpqd.com.br – (19) 3705-6186.

LSI TEC Associação do Laboratório de Sistemas Integráveis Tecnológico, CNPJ 03.018.444/0001-42, com sede na Cidade de São Paulo, Estado de São Paulo, na Rua Paes Leme, 524, Conjunto 95/96, 9º Andar, Pinheiros, CEP 05424-90 – Contatos: Artur Gasparetto Paiola - arturgp@lsitec.org.br ou contato@lsitec.org.br (contato alternativo).

9. Referencias externa (PCI-PTS)

PIN Transaction Security		
Referencia	**Documento**	**Localização**
Payment Card Industry Resources	Device Testing and Approval Program Guide	https://www.pcisecuritystandards.org/documents/PTS_Program_Guide_v1-4_March_2014.pdf
PCI Documents Library	Série de documentos de apoio	https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

10. Termo de confidencialidade e responsabilidade com a ABECS - Draft

TERMO DE CONFIDENCIALIDADE

Pelo presente Termo de Confidencialidade, a ABECS – Associação Brasileira das Empresas de Cartões de Crédito e Serviços, CNPJ 42.159.244/0001-61, com sede na Cidade de São Paulo, Estado de São Paulo, na Avenida Brigadeiro Faria Lima, n° 1485, 13º Andar, Torre Norte, Jardim Paulistano, CEP 01452-921, aqui representada na forma de seu Estatuto Social, e a entidade:

xxxxxx

Doravante referenciado por "Laboratório", têm entre si ajustada a celebração do presente Termo de Confidencialidade, a vigorar com as seguintes cláusulas e condições:

I - CONSIDERANDO:

(i) Que a ABECS, juntamente com os fabricantes de equipamentos e o Laboratório, definiram a partir do documento de requisitos de segurança para POS e PINPAD, elaborado pelo PCI Council, um documento próprio, com requisitos adicionais e datas aplicáveis somente ao Brasil;

(ii) O interesse geral do mercado em aumentar a segurança nas transações eletrônicas;

(iii) A busca por otimização de tempo e custo de certificação dos equipamentos nas credenciadoras;

(iv) O interesse da ABECS e suas Associadas em homologar laboratórios para a certificação de equipamentos segundo padrões definidos pelo PCI e pela ABECS no documento acima citado;

(v) Que os laudos bem como os relatórios detalhados emitidos pelo Laboratório deverão ter caráter estritamente confidencial e não deverão de modo algum serem exibidos em meio público e externo ao âmbito das pessoas jurídicas envolvidas, armazenados sem proteção ou cedidos a pessoas não-autorizadas.

As partes firmam o presente Termo de Confidencialidade, com o fim de assegurar que os dados e informações compartilhados sejam mantidos sob sigilo e que sejam utilizados exclusivamente para desenvolver serviços de testes de conformidade com os padrões publicados pela ABECS em complemento com o padrão publicado pelo

PCI Council de segurança dos dispositivos de captura de transações podendo também ser entendido como testes de violação.

Para fins do presente instrumento, serão utilizadas as seguintes definições:

a) PRODUTO: serviços de testes de conformidade com os padrões publicados pela ABECS em complemento com o padrão publicado pelo PCI Council de segurança dos dispositivos de captura de transações podendo também ser entendido como testes de violação;
b) ABECS Associação que representa as empresas de Cartões e Serviços no Brasil;
c) Informações Confidenciais: todos e quaisquer dados, informações, documentos e conhecimentos de natureza técnica e operacional divulgadas pelas Associadas ABECS, em qualquer meio em que se encontrem, estritamente relacionados ao PRODUTO, tais como especificações técnicas, operacionais e tecnológicas que o Laboratório venha a receber dos fabricantes de equipamentos e da ABECS para a realização de testes de Certificação de Segurança para Dispositivos de Captura de Senhas. Também considera-se como informação confidencial as técnicas e resultados obtidos nos testes de conformidade dos produtos com os padrões definidos pela ABECS.

II - CONFIDENCIALIDADE

II.1 - O presente Termo tem por objeto estabelecer as condições sob as quais as Associadas ABECS e o Laboratório poderão, entre si, dar conhecimento sobre determinadas Informações Confidenciais de cada uma das partes para os fins específicos e exclusivos de analisar a viabilidade do PRODUTO em cumprimento ao documento “Padrões de Segurança para Dispositivos de Captura de Transações”, publicado pela ABECS.

II.2 - As Informações Confidenciais deverão ser mantidas em sigilo, independentemente de conterem qualquer marca ou sinal indicativo indicando tratar-se de uma informação confidencial ou restrita.

II.2.1 - Não serão consideradas Informações Confidenciais aquelas que:
a) Sejam ou tornem-se de domínio público sem a violação deste Termo de Confidencialidade;
b) Estejam ou venham a estar disponíveis ao Laboratório livres de quaisquer restrições relativas ao seu uso e divulgação, desde que a fonte de tais informações não esteja sujeita a qualquer obrigação de sigilo;
c) Que tenham sido desenvolvidas de forma independente pelo Laboratório, sem a utilização direta ou indireta de quaisquer Informações Confidenciais

fornecidas para o desenvolvimento do PRODUTO considerando-se, porém, que informações resultantes dos testes efetuados deverão ser consideradas confidenciais, a não ser que haja a devida autorização por parte do demandante da atividade.

II.3 O Laboratório se obriga, por si e por seus administradores, empregados e terceiros contratados, a manter completo e absoluto sigilo sobre todas as Informações Confidenciais que receber ou tiver acesso, comprometendo-se a utilizá-las única e exclusivamente para viabilizar o PRODUTO. O Laboratório deverá fazer com que os seus administradores, empregados e terceiros contratados assinem um Termo de Confidencialidade ou documento equivalente que regulamente o recebimento e o uso das Informações Confidenciais em termos não menos restritivos do que aqueles aqui estabelecidos.

II.4 - É vedado ao Laboratório, incluindo seus administradores, empregados e terceiros contratados, a explorar, reproduzir, copiar, divulgar, revelar, ceder, comercializar ou doar, em proveito próprio ou de terceiros, qualquer das Informações Confidenciais.

II.5 - Cada uma das partes se obriga ainda a: (a) guardar em local seguro e fora do alcance de terceiros todos os meios que por qualquer forma contenham Informações Confidenciais e limitar o seu acesso apenas às pessoas que efetivamente necessitem conhecê-las em razão do desenvolvimento do PRODUTO; (b) não questionar nem disputar quaisquer direitos autorais ou de propriedade industrial sobre as Informações Confidencias da outra parte; e (c) não revelar a terceiros a existência, o conteúdo e as condições deste Termo, bem como do documento “Padrões de Segurança para Dispositivos de Captura de Transações“ ou de eventual contrato sobre o PRODUTO, que venha a ser firmado entre uma das Associadas ABECS e o Laboratório, sem a prévia e expressa autorização nesse sentido.

II.6 - Mediante a solicitação da ABECS ou de qualquer das Associadas ABECS, a qualquer tempo, ou no caso de término ou rescisão deste Termo de Confidencialidade, o que ocorrer primeiro, o Laboratório obriga-se a, no prazo máximo de 10 (dez) dias, devolver, inutilizar, destruir ou apagar, conforme o caso, todas e quaisquer notas, relatórios, fotocópias, rascunhos e quaisquer outros meios que contenham Informações Confidenciais, não podendo, de forma alguma, reter quaisquer cópias ou arquivos eletrônicos sem autorização expressa de quem as divulgou.

II.7 - Caso o Laboratório venha a ser obrigado por força de lei ou determinação de autoridade administrativa ou judicial a divulgar qualquer das Informações Confidenciais, deverá notificar a ABECS e/ou qualquer das Associadas ABECS envolvidas, de modo que possam tomar as medidas que reputarem cabíveis.

II.8 - Todas as Informações Confidenciais reveladas sob este Termo de Confidencialidade são e deverão permanecer de propriedade de quem as divulgou. Nenhuma licença ou direito sobre qualquer patente, *copyright*, marca, logomarca ou segredo de negócio será concedida ou transferida sob este Termo de Confidencialidade ou quando da revelação de quaisquer Informações Confidenciais.

II.9 – As obrigações de confidencialidade estabelecidas neste documento deverão ser observadas enquanto o mesmo viger e por 5 (cinco) anos, contados a partir do seu término ou rescisão.

III – DAS INSPEÇÕES DA ABECS

III.1 – Como legítima representante das suas Associadas, a ABECS poderá inspecionar as instalações e o *modus operandi* do Laboratório aplicado na execução do PRODUTO, de modo a garantir a qualidade e destreza confeccionadas na sua elaboração, em fiel consonância com o padrão de qualidade homologado pela ABECS, bem como o cumprimento das cláusulas e condições deste Termo de Confidencialidade. Caso o Laboratório não esteja atendendo aos requisitos, deverá ser advertido e perderá sua condição de laboratório homologado em caso de reincidência em um período inferior a 12 meses.

III.2 – A inspeção poderá se realizada a qualquer tempo, desde que respeitando prazo prévio de notificação ao Laboratório não inferior a 48 (quarenta e horas), salvo eventual outro ajuste formalizado entre as partes.

III.3 – A inspeção somente poderá ocorrer nas dependências e em relação aos procedimentos pertinentes ao objeto deste Termo de Confidencialidade.

IV – VIGÊNCIA

IV.1 - Este Termo de Confidencialidade entrará em vigor na data de sua assinatura e permanecerá em vigor pelo período em que o Laboratório estiver credenciado junto a Abecs ou até que as informações Confidenciais se tornem conhecidas e disponíveis ao grande publico, o que ocorrer primeiro.

V – CONDIÇÕES GERAIS

V.1 - O Laboratório será a o único responsável, por si, seus administradores, empregados, consultores e contratados, pela reparação de todo e qualquer dano, lesão ou prejuízo causado em relação à ABECS, suas Associadas ou terceiros em decorrência do descumprimento das disposições contidas neste Termo de Confidencialidade.

V.2 - O presente instrumento e todas as obrigações e direitos dele decorrentes não poderão ser cedidos, total ou parcialmente, por uma das partes a terceiros sem o prévio consentimento da outra parte.

V.3 – O presente instrumento obriga as partes, seus representantes legais, sucessores e cessionários autorizados.

V.4 - A omissão ou tolerância por qualquer das partes em exigir o estrito cumprimento dos termos e condições do presente Termo de Confidencialidade não constituirá novação ou renúncia dos direitos aqui estabelecidos, que poderão ser exercidos plena e integralmente a qualquer tempo.

V.5 - A inexequibilidade de qualquer condição ou cláusula deste Termo de Confidencialidade não invalida ou prejudica as demais que continuarão válidas e exequíveis.

V.6 - As partes elegem o foro Central da Comarca de São Paulo, Estado de são Paulo para dirimir, quaisquer controvérsias oriundas do presente Termo de Confidencialidade, com renúncia de qualquer outro, por mais privilegiado que seja.

E, estando assim justas e contratadas, as partes celebram este Termo em 2 (duas) vias de igual teor e forma, na presença de 2 (duas) testemunhas abaixo assinadas.

São Paulo, 30/09/2016.

_____

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CRÉDITO E SERVIÇOS

_____

xxx

Testemunhas

_____

xx

_____

xxx