Certificação de Segurança para Dispositivos de Captura de Senhas

Comitê de Segurança de Equipamentos Transacionais

Ano 2025

Versão 8.0

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

ÍNDICE

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

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.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

Manual_ABECS_v7	03/02/2015	Excluído o Item 6 (Recertificação)sendo acrescentado ao item 5. Renumerando 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.
Manual_ABECS_v		Atualizado o documento com relação as testes realizados. Removido o NDA ABECS, será tratado em outro documento. Removido o processo de certificação de laboratórios a ABECS, será tratado em outro documento sobre o tema. Removido o item 4.4.2 Auditorias Será tratado no novo documento sobre o tema credenciamento de laboratório. Alterado o fluxo 4.2. Fluxo de homologação de equipamentos, para contemplar a validação se o fabricante/representante é um Criado o item 4.2. Relação de Fabricantes/Representantes homologados

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 nos equipamentos de captura POS (point-of-sale) e Pin Pad (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 introdução no mercado para as instituições e credenciadoras.
No passado, os fornecedores de PED's tinham de passar por vários testes diferentes para atender aos requisitos de segurança de todo o sistema de meios de pagamentos globais e locais. Isto se tornou caro, e muitas vezes criou confusão nos critérios de avaliação. 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 inclui outras empresas, e o mesmo foi designado para criar e recomendar melhores práticas para a segurança de dados, a serem seguidas pelos estabelecimentos comerciais e processadoras que aceitam cartões como forma de pagamento, tendo como principal objetivo 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 DSS se aplica a toda e qualquer empresa que coleta, processa, armazena e transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão. Em linhas gerais, esta norma 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 cartões como gateways de pagamento. Também se aplica aos fabricantes que especificam e implementam dispositivos destinados à captura do número de identificação pessoal (PIN) s, sendo que para esses dispositivos é aplicado o PCI-PTS.

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

1.4.1 Visão Geral

No passado, o PED Security Requirements era supervisionado pelo JCB, MasterCard e VISA. Atualmente, através do PCI SSC, as cinco principais marcas mundiais de meios de pagamento (American Express, Discover, JCB, MasterCard e Visa) gerenciam as exigências de segurança do programa PTS, permitindo padronizar os requisitos dos dispositivos de segurança, as metodologias de testes e os processos de aprovação para PIN Transaction Security (PTS).
É prioridade estratégica para o PCI SSC padronizar as normas de segurança e garantir a continuidade do desenvolvimento dos 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.

Na parte lógica, são consideradas as características de segurança que incluem as capacidades funcionais que impeçam o acesso a dados dos terminais, como por exemplo, cópia da aplicação, acesso a chaves criptográficas e dados processados.

A gestão do PED deve ser 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 nas 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, seus critérios de avaliação e definição dos 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, tempo e complexidade das operações de meios de pagamentos.

3. Escopo

Equipamentos de captura de senha e/ou dados de cartão (podendo ser POS, Pin Pad's, entre outras soluções) homologados pelo PCI PTS e com certificado válido.

4. Periodicidade de revisões do documento

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

Revisão anual: Acontecerá sempre no mês de julho de cada ano e terá como finalidade promover a atualização de conteúdo.

Revisão dos Requisitos: Acontecerá a cada 6 meses após a data de lançamento e terá a finalidade de incluir, alterar ou excluir requisitos.

Revisão emergencial: Acontecerá sempre que for encontrada uma nova vulnerabilidade nos terminais.

5. Processo de certificação de equipamentos

5.1. Definição

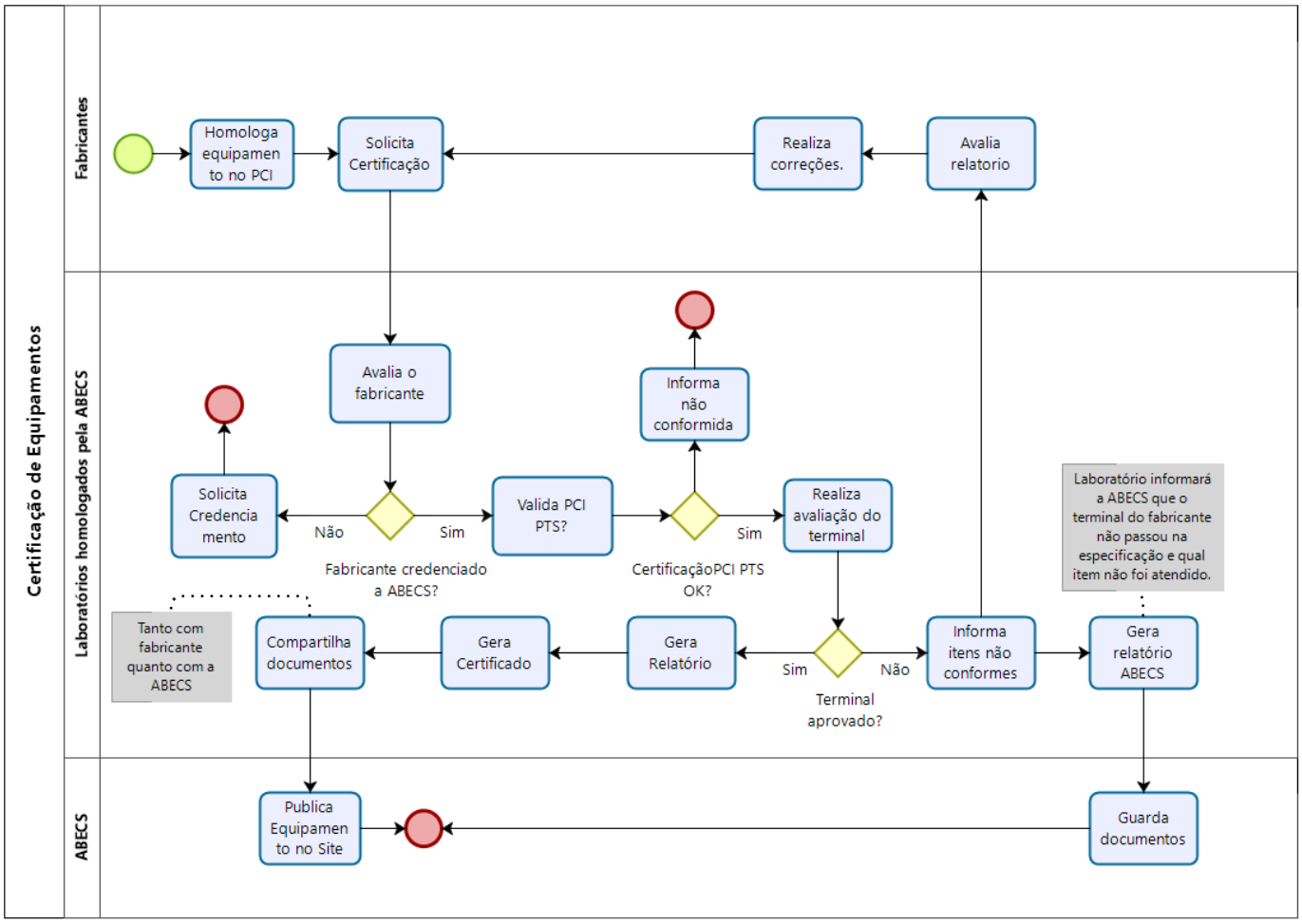
Estes processos contemplam os requisitos para os equipamentos, critérios de testes destes equipamentos, e controle de qualidade dos testes efetuados.

5.2. Relação de Fabricantes/Representantes homologados

Os fabricantes que por ventura queiram homologar os seus terminais deverão procurar a ABECS, os dados de contato estão no site da Instituição.
A ABECS fornecerá aos laboratórios credenciados a lista de fabricantes/representantes homologados credenciados e aptos a participarem do processo, além dos contatos da entidade caso algum fabricante/representante queira se credenciar.

5.3. 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.
Cabe ressaltar que a homologação de terminais só será realizada para fabricantes credenciados pela ABECS, caso contrário o laboratório deverá recusar a homologação e orientar o fabricante/representante a procurar a ABECS e se credenciar.
O fabricante deverá entregar 5 terminais ao laboratório para a realização das avaliações.



Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

6. Pré-requisito para Certificação

6.1. Fabricantes: Neste momento o fabricante poderá certificar a família (entende-se como família os terminais com periféricos, com ou sem impressora, com ou sem GPRS/WIFI/Bluetooth/3G entre outros) de terminais ou apenas um modelo. É necessário preparar 05 (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.
O fabricante deverá informar qual a versão do hardware e do firmware PCI do equipamento, além de disponibilizar os tipos de variações conhecido como wildcard, geralmente caracterizado pelos "x" na versão de hardware e firmware PCI homologado.

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

6.3. Laboratórios: Receber os terminais e realizar os testes dentro do prazo estipulado, caso haja alguma dúvida do laboratório em momento de análise caberá ao laboratório informar ao fabricante. Devendo o laboratório contactar a ABECS para que possam analisar e dar o devido direcionamento, todo esse processo não será contabilizado da "Hora Analista".
A tabela abaixo representa as horas destinadas à análise de um modelo de terminal.

Nome da tarefa	Duração	Hora Analista
Análise 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

7. Pré-requisito para Recertificação

7.1. Fabricantes:

7.1.1 - Alterações Hardware: Caso haja atualização do hardware que demande um DELTA PCI PTS deverá ocorrer uma nova avaliação/recertificação do terminal na ABECS.

7.1.2 - Alterações no Firmware PCI: Havendo alterações no core de segurança do firmware PCI o fabricante deverá enviar o release notes para a ABECS informando quais são os aspectos detalhados de segurança que foram alterados ou adicionados. A ABECS deverá encaminhar aos participantes um documento informando a vulnerabilidade encontrada e as recomendações do fabricante.

7.2. Recomendação ABECS: As recomendações ABECS só serão avaliadas se o hardware anterior apresentou as recomendações, caso haja a evolução do equipamento onde a recomendação tenha sido implementada essa deverá ser avaliada. Porém,caso o hardware na sua avaliação incial não contemplava as recomendações ABECS esse não deverá ser um item blocante na reavaliação. Os resultados da avaliação dos itens de recomendação devem constar do relatório detalhado. Deverá constar no certificado os dados do hardware e do firmware PCI.

7.3. Do processo de recertificação:
A recertificação deverá ocorrer preferencialmente no mesmo laboratório que foi realizada a certificação da versão PCI anterior. Caso contrário, o fabricante deverá compartilhar o relatório da análise do laboratório anterior para o novo laboratório, além das demais informações que o laboratório entender como necessárias. A versão da especificação ABECS a ser seguida será a vigente do primeiro terminal avaliado anteriormente.É possível certificar o terminal de acordo com uma versão mais recente da especificação ABECS, entretanto será tratado como uma nova certificação.

7.4. Laboratório: Receber os terminais e realizar os testes dentro do prazo estipulado.
O prazo a ser seguido deverá ser do item 5.3.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

7. Requisitos

7.1.Equipamentos

7.1.1 Requisitos ABECS 01 – Segurança Física

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 forma 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 deverá ser neutralizada.
Os sensores de segurança por pressão quando possível devem ser protegidos por outro sistema / mecanismo de segurança.
Os circuitos sensíveis que estejam no layer superficial da PCB do teclado dos equipamentos devem ser protegidos pela Mesh, essa exigência não se aplica a teclados touchscreen.
Soluções de backlight ou lightguide ou soluções adversas, sejam elas para outras finalidades, mas que estejam no teclado não deverão fragilizar o equipamento ao ponto de propiciar facilidades na obteção dos dados da senha do portador do cartão.

Obrigatório todo terminal com teclado físico ter a Mesh de proteção no teclado, com no mínimo duplo layer. A mesh deverá proteger não só as os circuitos de segurança bem como os contatos das teclas do teclado, caso contrário não será aceito, soluções com as da imagem abaixo não serão mais aceitas.

Imagem 1 – Foto ampliada de uma mesh de duplo layer sem proteger os contatos do teclado.

***Ressaltamos que:** Caso o equipamento seja submetido a análise do laboratório e esse conte com uma nova solução de segurança melhor ou equivalente ao requisito em questão o laboratório deverá submeter a ABECS tal solução afim de que o Comitê avalie a solução e formalize ao laboratório se a solução atende ou não ao requisito. O Comitê de Segurança de Equipamentos Transacionais deverá analisar se cabe uma atualização do requisito em questão para que novas demandas de certificação similares as que forem sendo submetidas à certificação possam ser avaliadas pelo (s) laboratório(s) sem a necessidade de acionarnovamente o Comitê, para que os prazos de avaliação sejam respeitados.

Critério de avaliação*:

Neste item, os laboratórios considerarão apto o equipamento quando:

1. Não for possível burlar a segurança 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. Usar no máximo 5 equipamentos por modelo.
3. Avaliar os sistemas de segurança e os meios de proteção adicionais aos circuitos de segurança por pressão
4. Avaliar a quantidade de layers das mesh aplicadas nos circuitos de segurança quando utilizado mesh.
5. Caso o fabricante opte por uma solução diferente da Mesh/Manta de duplo layer (no mínimo) deverá essa solução ter o mesmo nível de segurança ou superior ao da manta/mesh e deverá ser submetida ao crivo do GT responsável para análise e apoio ao laboratório.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

7.1.2 Requisitos ABECS 02 – Proteção de cabos de comunicação do Pin Pad

Tipo:
Físico.

Data de início de validade:
Imediata

Descrição:

O Pin Pad 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.

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

Critério de avaliação:

1. Neste item, os laboratórios devem considerar 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).

Exceção:

1. Este item não deve ser aplicado a Pin Pad's que sejam unicamente wireless, bluetooth, wifi direct ou qualquer outra comunicação sem fio.
2. Deve o laboratório informar no laudo que o item não se aplica por conta do meio de comunicação do Pin Pad ao dispositivo transacional ser wireless.

7.1.3 Requisitos ABECS 03 – Identificação única de equipamentos

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 de Testes.**
2. O número de série interno gravado na memória do terminal deve ser idêntico ao número gravado na etiqueta externa.

Recomendação ABECS:

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.

7.1.4 Requisitos ABECS 04 – Resposta de Violação do Terminal - Tamper

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 que sejam pertinentes ao fluxo transacional;
-Remover todos os softwares instalados que sejam pertinentes ao fluxo transacional com exceção ao Sistema Operacional;
-Terminal deve ficar inoperante para transações financeiras seja através de carteiras digitais, transações via QrCode, EMV, contactless, tarja e digitada, além do bloqueio da função do teclado para captura de PIN (senha do portador do cartão).
-Todo terminal com display em Tamper deverá ficar com alerta constante de que a sua segurança foi violada, independente do tipo de terminal e uso, devendo esse alerta ser realizado de forma contínua, e não deve ser possível a sua remoção até que ocorra uma intervenção técnica do fabricante, ou de um laboratório credenciado por ele.
-Para terminais Smart's (Android) quando em tamper deverão ter o mesmo comportamento de um terminal não Smart, não sendo possível a sua utilização.
-Não poderá ter nos terminais meio que não seja o do laboratório do fabricante forma para remoção de tamper.
- Novo – Não poderá haver no terminal meio tanto lógico quanto físico que permita a remoção do estado de tamper. A remoção do estado de tamper deverá ser realizada somente em local seguro do fabricante.
- O processo de tamper deverá ocorrer não só nos produtos que estejam com a versão de produção, mas também nas versões de demonstração, default certification, engenharia, mockup, e qualquer outra versão de teste ou homologação.

- Recomendação ABECS: 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 os itens descritos anteriormente estão sendo atendidos em sua plenitude.
2. Quando um terminal estiver em tamper somente o fabricante deverá ser o responsável pela remoção do Tamper do terminal, devendo o fabricante prover ferramental e documentação para o laboratório validar que nenhuma outra aplicação possa mudar o status do equipamento.

Ressaltamos que: Caso o equipamento seja submetido a análise do Comitê e esse conte com uma nova solução de segurança melhor ou equivalente ao requisito em questão o laborartório deverá sobmeter a ABECS tal solução afim de que o Comitê avalie a solução e formalize ao laboratório se a solução atende ou não ao requisito. O Comitê deverá analisar se cabe uma atualização do requisito em questão para que novas demandas de certificação com soluções similares as que forem sendo aprovadas no Comitê possam ser

avaliadas pelo (s) laboratório(s) sem a necessidade de novo acionamento do Comitê, para que os prazos de avaliação sejam respeitados..

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

7.1.5 Requisitos ABECS 05 – Assinatura de Aplicação

Tipo: Lógico

Data de início de validade:
Imediata

Descrição:

Todo software carregado no dispositivo de captura deverá ser assinado digitalmente pelo fabricante do dispositivo com a possibilidade de também ser assinado digitalmente pelo fabricante do software e pelo proprietário do equipamento.

O terminal com perfil de produção não poderá ter seu sistema operacional substituído por um de debug.

- Recomendação ABECS: Para terminais com Android, onde seja possível a utilização em loja privada de aplicativos, o fabricante tenha distinção de certificados sendo um para aplicação financeria e outro para as aplicações de loja, devendo a assinatura de aplicação financeira ter acesso a todos os recursos padrões de uma aplicação do tipo, e para aplicações de Loja de Aplicativos, ser menos permissiva.

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.
3. Se há como converter o terminal produtivo para um terminal Debug ou diminuir o nível de segurança do software do terminal que permita a instalação indevida de aplicações ou mesmo a instalação de um outro sistema operacional mais frágil.
4. Caso o fabricante informe que atende a Recomendação para terminais Androids, deverão apresentar documentação que comprove tal comportamente, e se possível, mostrar os sistema de assinatura e seus sistemas de segregação de função.

Os fabricantes deverão entregar os meios necessários para os testes de assinatura de aplicação.

7.1.6 Requisitos ABECS 06 – Segurança Lógica

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;
- Os terminais não poderão ter habilitado, em ambiente produtivo, as interfaces de comunicação JTAG/I2C/UART entre outros que possam trazer risco de captura de dados transacionais ou mesmo que possam ocasionar em utilização indevida do equipamento.
- Low batery: O software não deverá desativar as funções de segurança, não importando se a alimentação é externa ou não e para quaisquer níveis de carga das baterias interna e externa.
- Impossibilitar que em terminais de produção seja removido qualquer tipo de software instalado por portas de comunicação (USB, SERIAL entre outras) em equipamentos produtivos, ou com certificado de produção, sendo exceção os terminais para desenvolvimento de aplicação.

Critério de avaliação:

Os laboratórios devem verificar se existem condições de execução das ações acima, caso contrário deverá evidenciar no laudo que irá para a ABECS a impossibilidade de exploração do(s) item(s). Devem contar com a colaboração do fabricante.

Possíveis cenários para obtenção de evidências:

a) Com o terminal em TAMPER, tentar remover o TAMPER do equipamento.

b) Com o terminal ainda ativo, testar a viabilidade de conseguir obter dados de transações.

c) Evidenciar a obtenção de qualquer informação que possa ser utilizada para fraude.

d) Qualquer outro cenário que o laboratório encontre que vislumbre a exploração de potenciais ameaças.

Observação: Caso haja dúvidas com relação aos dados coletados o laboratório deverá solicitar à ABECS reunião com o time técnico para a validação.

7.1.7 Requisitos ABECS 07 – Segurança das Leitoras de Cartão

Tipo:
Físico

Data de início de validade:
Imediata para dispositivos de captura que possuam a certificação **PCI-PTS válida** .

Descrição:
Não deverá ser possível o acesso à leitora de cartão, 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.
- Recomendação ABECS: Que as leitoras de chip tenham em seus componentes plásticos meios que detectem perfuração ou acesso indevido, sendo que ao detectar tais ações maliciosas o sistema de TAMPER deverá ser acionado.

7.1.8 Requisitos ABECS 08 – Leitora Contactless

Tipo:
Físico

Data de início de validade:
Opcional a critério do fabricante – Não mandatório.

Descrição:
A crescente utilização de cartões contactless e dispositivos móveis dotados de tecnologia NFC, vem trazendo questionamentos por parte dos portadores de cartão sobre a validação do valor informado na transação.

Sugere-se que:

1. **O usuário deverá poder visualizar o valor da transação de forma fácil antes de utilizar o leitor contactless;**
2. **Recomenda-se que a leitora de cartões contactless esteja presente na tela do terminal e com a devida sinalização.**

Observação esse é um requisito opcional devendo apenas constar que o requistio ABECS 8 foi atendido ou não nos relatórios enviado a ABECS e aos fabricantes.

Critério de avaliação:
O laboratório deverá informar se o terminal atende ou não ao requisito.

7. Relatórios e Certificados gerados pelos laboratórios

Quando o terminal for reprovado, o relatório completo deverá ser enviado apenas ao fabricante. Porém, o laboratório deverá enviar para registro na ABECS um relatório parcial informando que o equipamento do fabricante não foi aprovado e qual requisito não atendido. Para terminais aprovados será necessário enviar os relatórios da seguinte forma:

A – Relatório detalhado: Envio apenas ao fabricante do terminal.
B – Relatório simplificado junto com o certificado de aprovação do terminal: Envio apenas à ABECS e ao fabricante.

Em todos os relatórios deverão ter as seguintes informações:

- Fabricante;
- Modelo do terminal cadastrado no PCI;
- Hardware e firmware reference do terminal testado;
- Versão do PCI do equipamento;
- Assinatura do responsável pelo teste.

Importante:

- O relatório 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.

Caso o laboratório forneça um certificado, no certificado deverá constar as seguintes informações:

- Fabricante;
- Modelo do terminal cadastrado no PCI;
- Hardware e firmware reference do terminal testado;
- Versão do PCI do equipamento;
- Assinatura do responsável pelo teste.

A ABECS assim que receber dos laboratórios os documentos que atestam que o terminal está apto terá o prazo de 15 dias uteis para atualizar o site com a informação do terminal e do fabricante.

O prazo poderá ser prorrogado caso haja inconsistência na documentação enviada.

8.Laboratórios Homologados

Os laboratórios certificados para avaliação de segurança do Hardware estão no “Guia de laboratórios credenciados da ABECS", disponível no site oficial da ABECS.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

9. Referências externa (PCI-PTS)

PIN Transaction Security		
Referência	**Documento**	**Localização**
PCI Documents Library	Série de documentos de apoio	https://www.pcisecuritystandards.org/document_library/

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br

10. Guia de credenciamento de novos laboratórios

Caso seja de interesse de alguma empresa pública ou privada atuar de forma parceira a ABECS como um dos laboratórios certificados para avaliação de segurança do Hardware, deverá avaliar se segue as diretrizes do “Guia solicitação de credenciamento de laboratórios da ABECS”, disponível no site oficial da entidade.

11. Termo de confidencialidade e responsabilidade com a ABECS

O termo de confidencialidade encontra-se no site da ABECS.

Rua Elvira Ferraz, 250, 4º andar, conj. 411
São Paulo, SP

11 3296-2750

www.abecs.org.br