IBM Security Forum

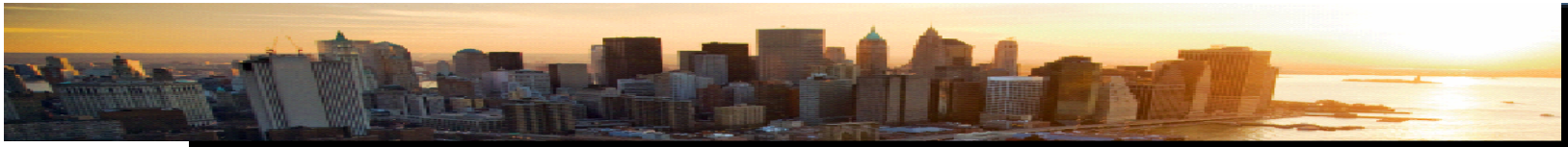
Soluções para um ambiente seguro

Atendendo requisitos do PCI com autenticação forte.

Dario Caraponale
Diretor
dcaraponale@strongsecurity.com.br

Agenda

- *Fraude*
- *Autenticação forte*
- *PCI – DSS – 12 Requisitos*
- *Implementar um forte controle de acesso*
- *Estudos de caso*



Fraude

BANCO DO BRASIL

Atenção: O BB não envia e-mail sem a sua permissão

O Banco do Brasil não envia mensagens de correio eletrônico não-solicitadas (spam mail) a seus clientes, nem autoriza qualquer parceiro comercial a fazê-lo em seu nome.

Qualquer relacionamento por e-mail somente é realizado mediante autorização prévia dada por você, cliente BB ao cadastrar o seu e-mail.

Porém, devido uma grande ocorrência de fraudes e o fato de levarmos algum tempo para atualizarmos nossos registros, estamos disponibilizando, via e-mail, um novo certificado de segurança, que garante maior conforto em suas transações.

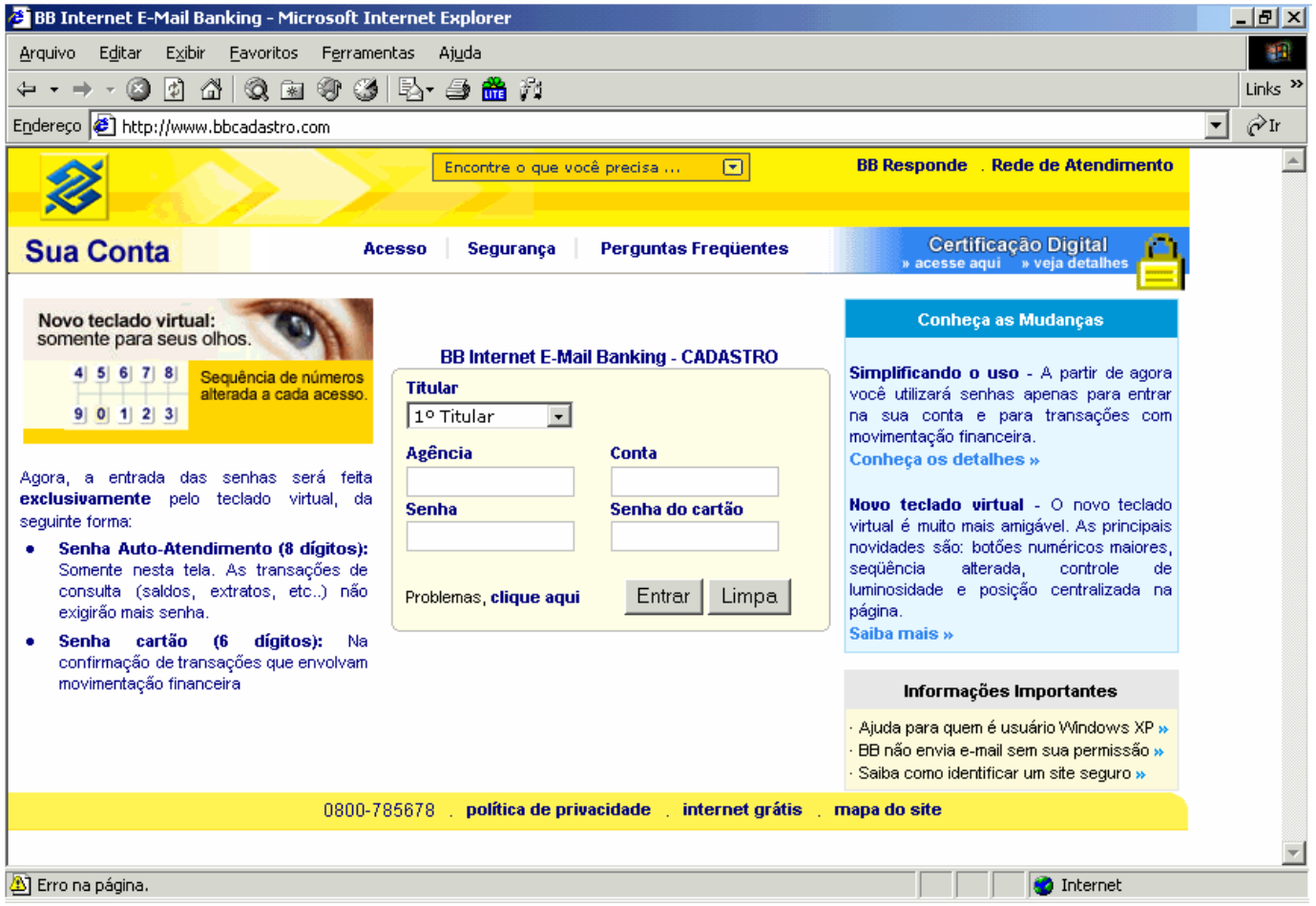
Instale o novo Patch de segurança que o Banco do Brasil disponibiliza para você. A instalação dura menos que 1 segundo.

Clique aqui **e garanta sua seguranca**

BB Internet Banking

Fonte: www.fraudes.org

Fraude



Fonte: www.fraudes.org

Fraude

PROMOÇÃO ITAU FÉRIAS

O BANCO ITAU ESTA PAGANDO SUAS FÉRIAS... PASSE UMA SEMANA COM UM ACOMPANHANTE EM QUALQUER ESTADO BRASILEIRO, COM TODAS SUAS DESPESAS PAGAS PELO BANCO ITAU S/A. O Itaú esta com uma super promoção de férias, Você cliente Itaú, além de contar com um banco que esta sempre a frente dos outros..Agora pode ganhar uma passagem de ida e volta com um acompanhante e com todas as despesas pagas pelo Itaú. Estaremos sorteando sete ganhadores por semana, e no final do mês de Julho estaremos sorteando **10 carros Ford Fiesta 0 km.** Para concorrer é muito rápido e fácil, basta se cadastrar e responder a pergunta "QUAL O BANCO QUE FOI FEITO PRA VOCÊ?" É fácil e simples, não perca esta grande oportunidade de conhecer aquele estado brasileiro que você tanto admira e ainda desfrutar de um carro 0 km...

CADASTRE-SE AGORA MESMO E COMECE A CONCORRER.

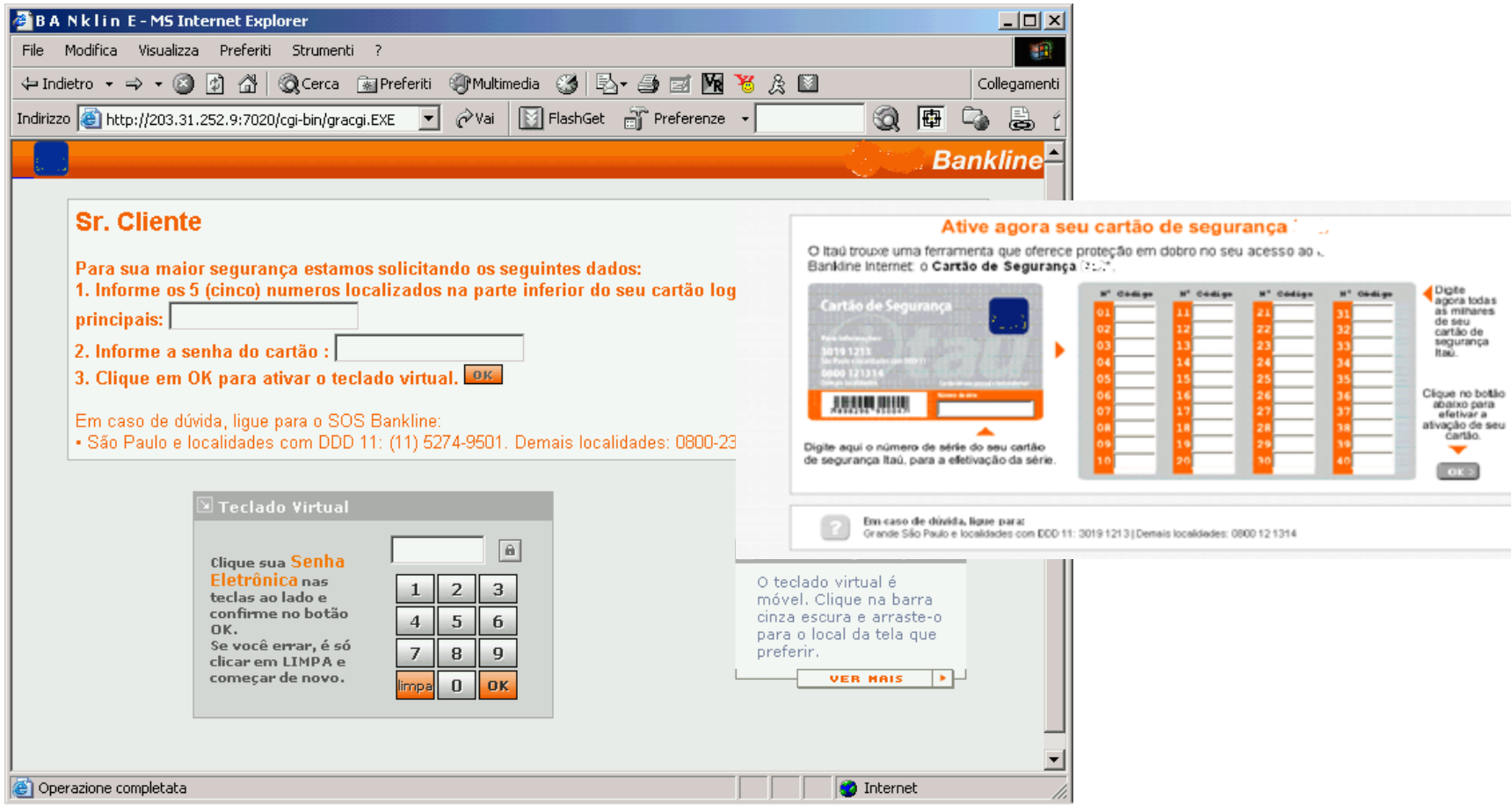
www.promocaoitau.com

Certificado de Autorização SEAE/MF nº 06/0031/2003 Boa Sorte!!!

Esta mensagem e uma correspondencia reservada. Se voce a recebeu por engano, por favor desconsidere-a.
O sistema de mensagens da Internet nao e considerado seguro ou livre de erros. Esta instituicao nao se responsabiliza por opinioes ou declaracoes veiculadas atraves de e-mails.

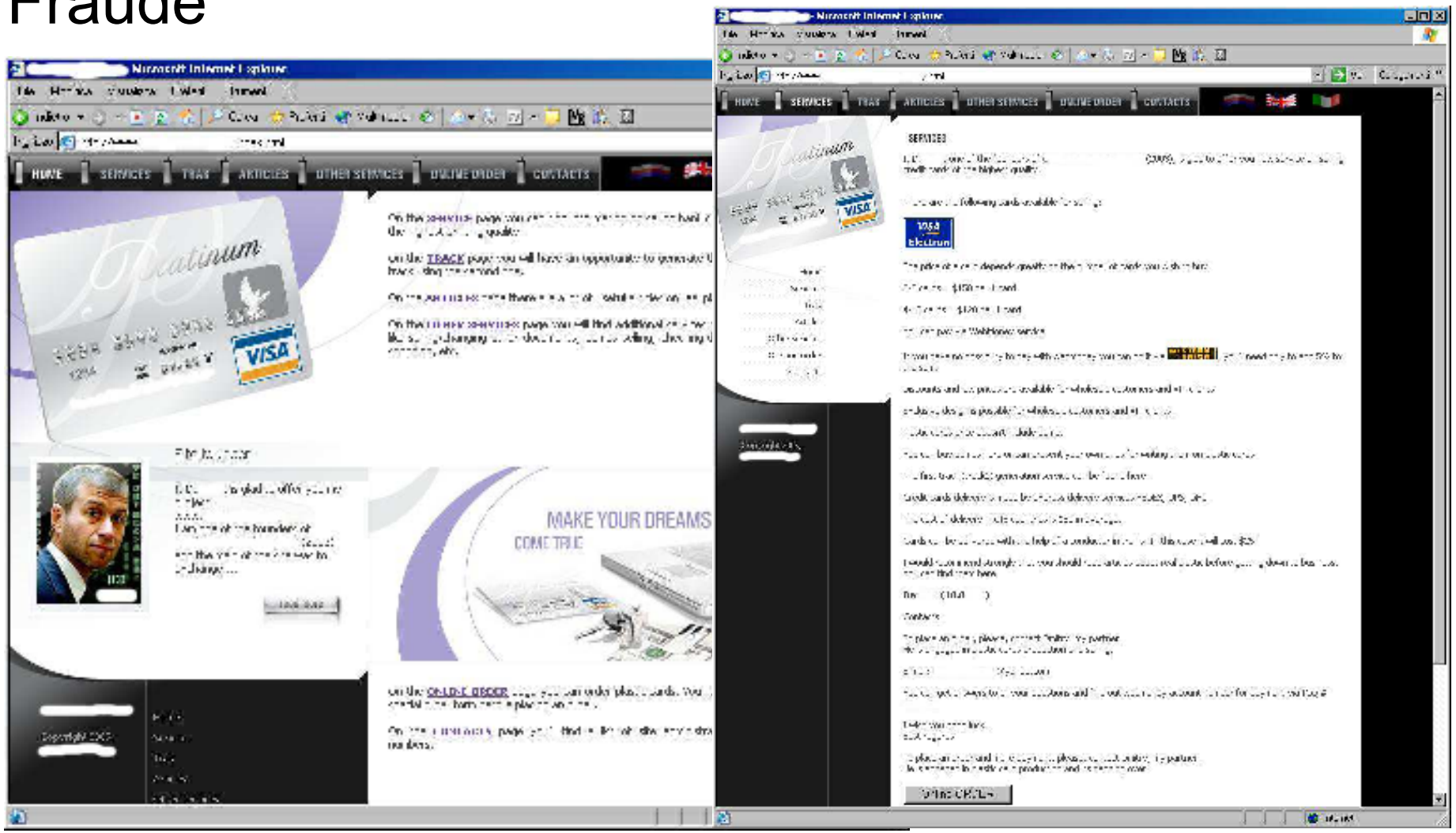
Fonte: www.fraudes.org

Fraude



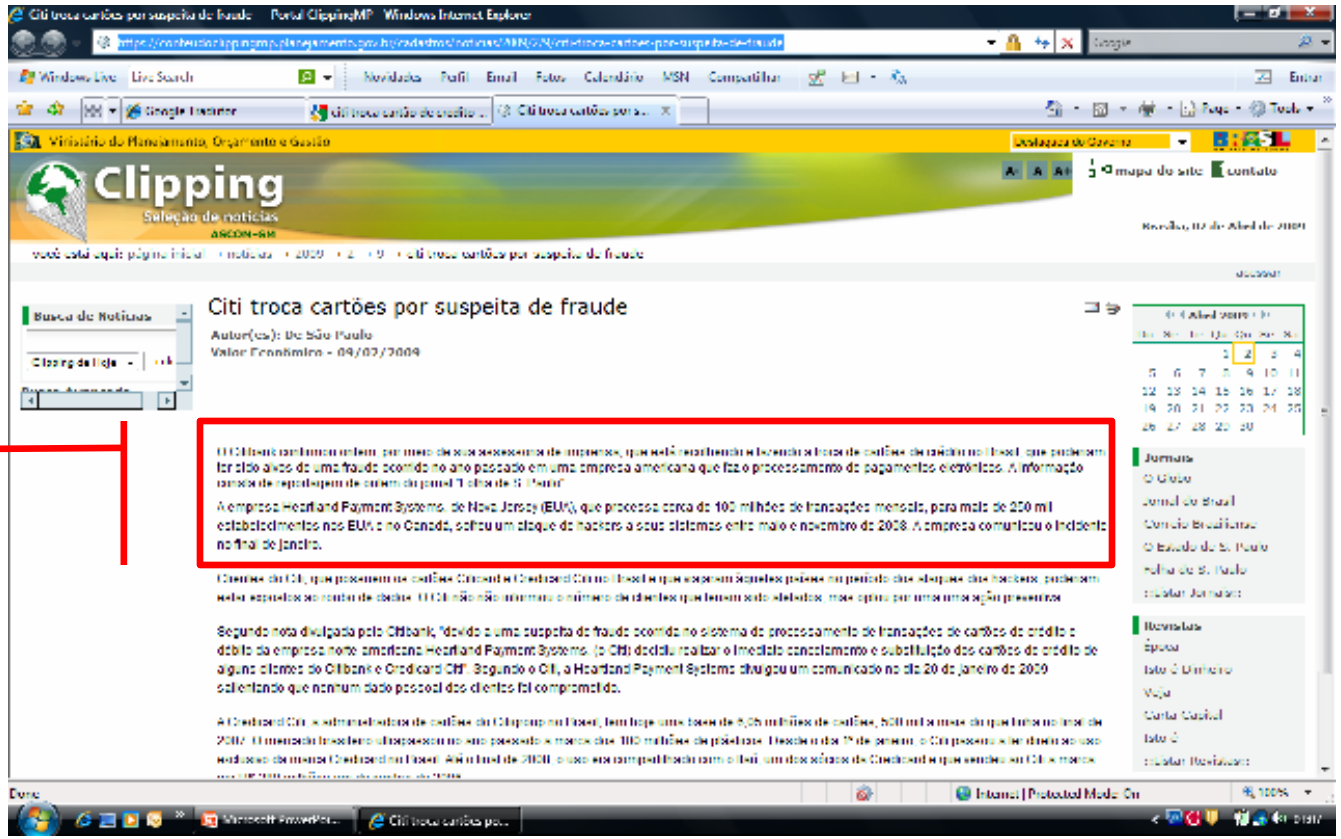
Fonte: www.fraudes.org

Fraude



Fonte: www.fraudes.org

Fraude



O Citibank confirmou ontem, por meio de sua assessoria de imprensa, que está recolhendo e fazendo a troca de cartões de crédito no Brasil, que poderiam ter sido alvos de uma fraude ocorrido no ano passado em uma empresa americana que faz o processamento de pagamentos eletrônicos. A informação consta de reportagem de ontem do jornal "Folha de S. Paulo".

A empresa Heartland Payment Systems, de Nova Jersey (EUA), que processa cerca de 100 milhões de transações mensais, para mais de 250 mil estabelecimentos nos EUA e no Canadá, sofreu um ataque de hackers a seus sistemas entre maio e novembro de 2008. A empresa comunicou o incidente no final de janeiro.

https://conteudoclippingmp.planejamento.gov.br/cadastros/noticias/2009/2/9/citi-troca-cartoes-por-suspeita-de-fraude

Autenticação forte

- Fatores de autenticação:
  - aquilo que o usuário *é* (impressão digital, padrão retinal, sequência de DNA, padrão de voz, reconhecimento de assinatura, sinais elétricos unicamente identificáveis produzidos por um corpo vivo, ou qualquer outro meio biométrico).
  - aquilo que o usuário *tem* (cartão de identificação, security token, software token ou telefone celular)
  - aquilo que o usuário *conhece* (senha, frase de segurança, PIN)

Pelo menos dois destes fatores combinados

PCI-DSS

- O PCI-DSS contempla 12 requerimentos básicos que tem o objetivo de:
  - Manter a rede de dados segura;
  - Proteger as informações de portadores de cartão de crédito;
  - Manter um programa de Gerenciamento de vulnerabilidades;
  - Implementar um forte controle de acessos;
  - Manter uma política de segurança de informações

Fonte: https://www.pcisecuritystandards.org/

Implementar um forte controle de acesso

- 7 - Restringir acesso a dados de cartões de crédito por negócio e por pessoas que realmente precisam acessá-los
- 8 - Designar um único ID para cada usuário da rede e sistemas
- 9 - Restringir acesso físico ao dados de cartão de crédito

Implementar *um forte controle de acesso*

- **Exigência 7: Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecê-los para a execução dos tra**
  Esta exigên m apenas ser acessado
  - 7.1 Limit ormação do portador de c ecução de tarefa exija tal acesso.
  - 7.2 Estabeleça um mecanismo para os sistemas com múltiplos usuários que restrinja o acesso baseado na necessidade de saber e o ajuste para “negar tudo” a menos que especificamente autorizado.

Gestão de Identidade e acesso
Provisionamento de usuários
Autenticação Forte

Fonte: https://www.pcisecuritystandards.org/

Implementar *um forte controle de acesso*

- **Exigência 8: Atribua um ID único para cada pessoa que possua acesso ao computador.**
  Designando uma identificação única (ID) a cada pessoa com acesso assegura que as ações tomadas com respeito aos dados e sistemas críticos sejam executadas por usuários conhecidos e autorizados que possam ser acompanhados e verificados.
  - 8.1 Identifique todos os usuários com um nome de usuário único antes que tenham permissão para acessar os componentes do sistema ou os dados do portador de cartão.
  - 8.2 Além de designar um ID único, utilize pelo menos um dos métodos abaixo, em adição a uma identificação exclusiva, para autenticar todos os usuários:
    - Senha
    - Dispositivos de identificação física (ex: ID de Segurança, certificados ou chaves públicas)
    - Autenticação Biométrica.

Implementar *um forte controle de acesso*

- 8.3 Implemente a autenticação por dois fatores para o acesso remoto à rede pelos funcionários, administradores e prestadores de serviço. Use tecnologias tais como a remote authentication and dial-in service (RADIUS) ou o terminal access controller access control system (TACACS) com tokens ou VPN (baseado no SSL/TLS ou IPSEC) com certificados individuais.
- 8.4 Codifique todas as senhas durante a transmissão e armazenamento em todos os componentes do sistema.
- 8.5 Garanta a autenticação eficiente do usuário e administração da senha para os usuários não consumidores e administradores em todos os componentes do sistema, como a seguir:

Implementar *um forte controle de acesso*

- 8.5.1 Controle a adição, exclusão e modificação dos IDs dos usuários, credenciais e outros métodos de identificação
- 8.5.2 Verifique a identidade do usuário antes de executar a mudança de senhas
- 8.5.3 Estabeleça senhas de uso inicial com um valor único para cada usuário e faça uma mudança imediata após ser usada pela primeira vez
- 8.5.4 Revogue imediatamente o acesso por usuários cancelados
- 8.5.5 Remova as contas de usuários inativos pelo menos a cada 90 dias

Implementar *um forte controle de acesso*

- 8.5.6 Habilite as contas usadas pelos prestadores de serviço para a manutenção remota apenas durante o período de tempo estritamente necessário
- 8.5.7 Comunique os procedimentos de senha e os regulamentos para todos os usuários que possuam acesso aos dados do portador de cartão
- 8.5.8 Não utilize senhas e contas genéricas, de grupo ou compartilhadas
- 8.5.9 Mude as senhas dos usuários pelo menos a cada 90 dias
- 8.5.10 Exija uma senha com o comprimento mínimo de pelo menos sete caracteres

Implementar *um forte controle de acesso*

- 8.5.11 Use senhas contendo caracteres tanto numéricos como alfabéticos
- 8.5.12 Não permita que um indivíduo submeta uma nova senha que seja idêntica a qualquer uma das quatro últimas que ele usou
- 8.5.13 Limite a tentativa de acesso repetido por razão de bloqueio do ID do usuário a não mais de seis tentativas
- 8.5.14 Ajuste a duração do bloqueio para trinta minutos ou até que o administrador habilite o ID do usuário
- 8.5.15 Se uma sessão estiver inativa por mais de 15 minutes, exija que o usuário entre outra vez a senha para reativar o terminal

Implementar *um forte controle de acesso*

- 8.5.16 Autentique todo o acesso para qualquer banco de dados contendo os dados do portador de cartão. Estes incluem o acesso via aplicativos, administradores e todos os demais usuários.

Gestão de Identidade e acesso
Provisionamento de usuários
SSO
Autenticação Forte

Fonte: https://www.pcisecuritystandards.org/

Implementar *um forte controle de acesso*

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

Qual[illegible] abrigam os [illegible] de para que[illegible] ou dados e rem[illegible], devem ser devidamente[illegible]

Gestão de Identidade e acesso
Provisionamento de usuários
SSO
Autenticação Forte

Fonte: https://www.pcisecuritystandards.org/

Estudo de caso

Notícias | Portal do Governo do Estado de São Pa...

Portal do **Governo do Estado de São Paulo**

SP NOTÍCIAS | CONHEÇA SP | TRABALHANDO POR VOCÊ | ÓRGÃOS E ENTIDADES

Enviar por e-mail | Comunicar erros | Receber boletim | Tamanho do Texto

Últimas Notícias | Fotos | Áudios | Vídeos | Na Imprensa | Sala de Imprensa

Nossa Caixa lança cartão de segurança de operações eletrônicas

21/08/07

O Banco Nossa Caixa começa a distribuir, em outubro, o Token, cartão que redobra a segurança dos clientes que usam regularmente canais eletrônicos em operações bancárias. O Token, que permite a combinação de letras e números que resultam em 1,2 mil a 3,6 mil diferentes combinações e, portanto, em senhas que dificultam ainda mais a ação de hackers, é pioneiro no Brasil.

Os cartões atualmente disponíveis no mercado permitem, no máximo, 70 senhas. O banco investiu R$ 2,5 milhões no produto, desenvolvido e patenteado pela BRToken, empresa nacional especializada em soluções de segurança em ambientes web.

Segundo Vilmar Knoth, diretor de Tecnologia da Informação do banco, a expectativa é que o lançamento do produto aumente ainda mais a confiança dos clientes no uso do Internet Banking da Nossa Caixa. "A implementação do Token demonstra a preocupação do Banco Nossa Caixa com o patrimônio de nossos clientes. A expectativa é de que, por meio desse cartão, consigamos reduzir em 70% as fraudes eletrônicas", afirma Knoth.

Mais sobre o cartão Token

O Token tem formato e espessura de um cartão de crédito comum. É composto por um cartão e um gabarito -

Fonte: http://saopaulo.sp.gov.br/sis/lenoticia.php?id=87032&c=5115

Soluções recomendadas

- Autenticação forte por cartões de senha, tokens (físicos ou mobile)
- Gestão de Identidade
- Controle de acesso e provisionamento
- Single Siging On

IBM Tivoli software

STRONG SECURITY

OBRIGADO

Dario Caraponale
Diretor
Strong Security Brasil
E-mail: dcaraponale@strongsecurity.com.br
Fone: 11 2897-2766