

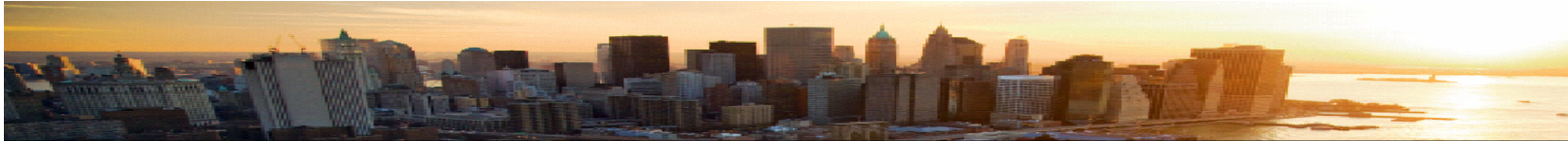


IBM Security Forum
Soluções para um ambiente seguro

Atendendo requisitos do PCI com
autenticação forte.

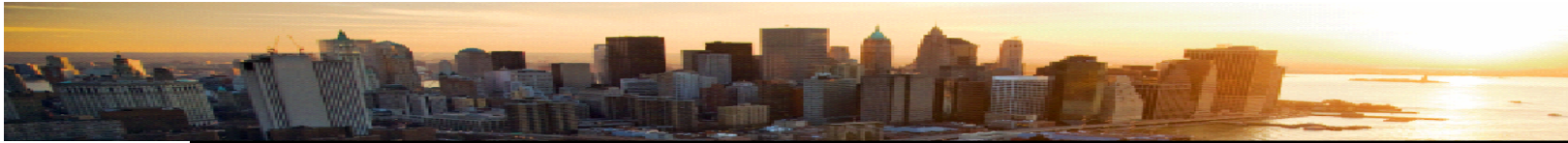
Dario Caraponale
Diretor

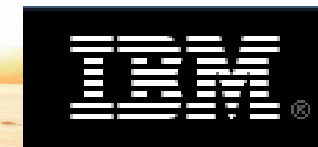
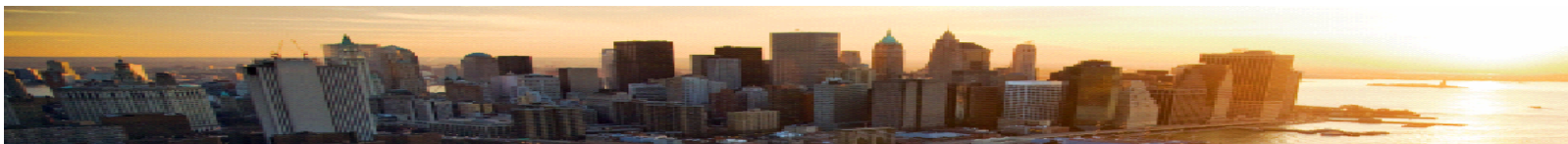
dcaraponale@strongsecurity.com.br



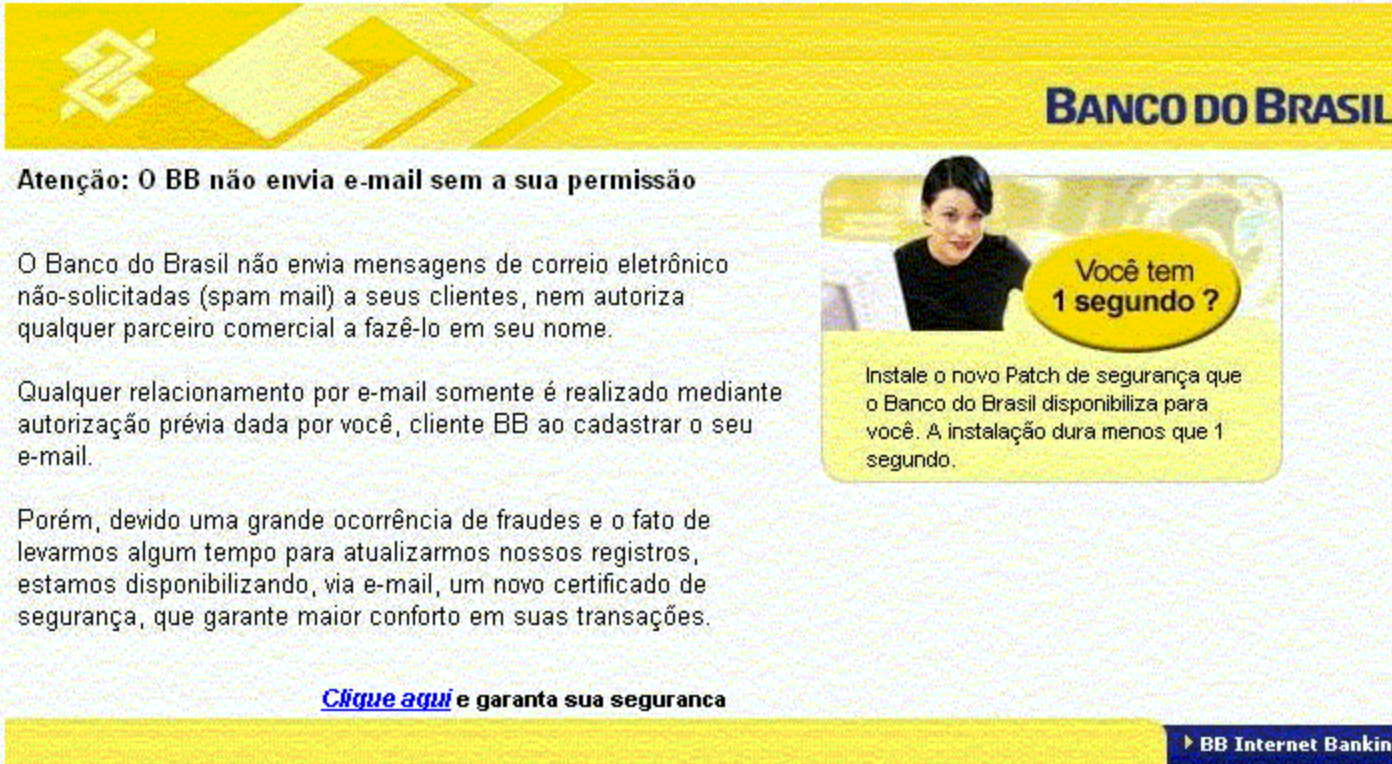
Agenda

- 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.

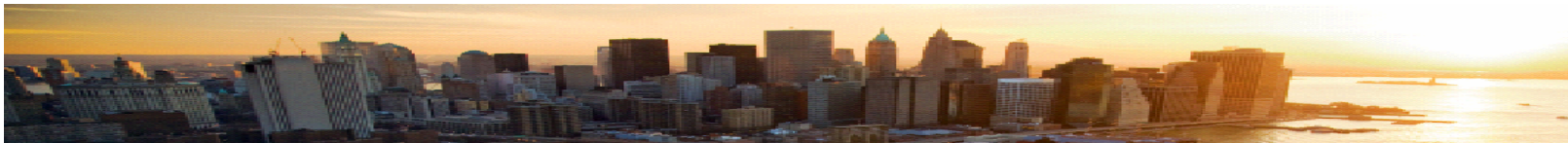
[Clique aqui](#) e garanta sua segurança

Você tem 1 segundo ?

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

▶ BB Internet Banking





Fraude

BB Internet E-Mail Banking - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://www.bbcadastro.com>

Encontre o que você precisa ... **BB Responde** . Rede de Atendimento

Sua Conta Acesso | Segurança | Perguntas Frequentes **Certificação Digital**
» acesse aqui » veja detalhes

Novo teclado virtual: somente para seus olhos.
4 5 6 7 8 Sequência de números alterada a cada acesso.
9 0 1 2 3

BB Internet E-Mail Banking - CADASTRO

Titular
1º Titular

Agência

Conta

Senha

Senha do cartão

Problemas, [clique aqui](#)

Conheça as Mudanças

Simplificando o uso - A partir de agora você utilizará senhas apenas para entrar na sua conta e para transações com movimentação financeira.
[Conheça os detalhes »](#)

Novo teclado virtual - O novo teclado virtual é muito mais amigável. As principais novidades são: botões numéricos maiores, sequência alterada, controle de luminosidade e posição centralizada na página.
[Saiba mais »](#)

Informações Importantes

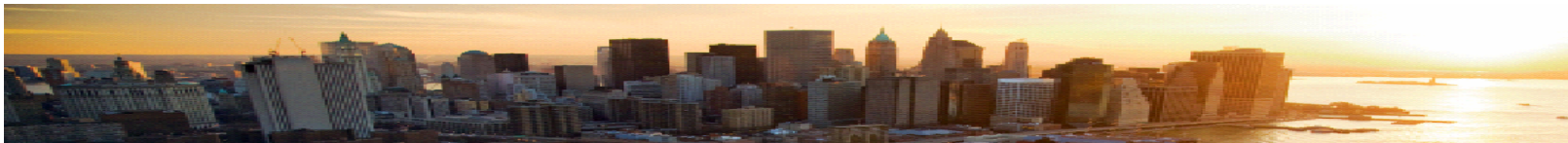
- [Ajuda para quem é usuário Windows XP »](#)
- [BB não envia e-mail sem sua permissão »](#)
- [Saiba como identificar um site seguro »](#)

0800-785678 . [política de privacidade](#) . [internet grátis](#) . [mapa do site](#)

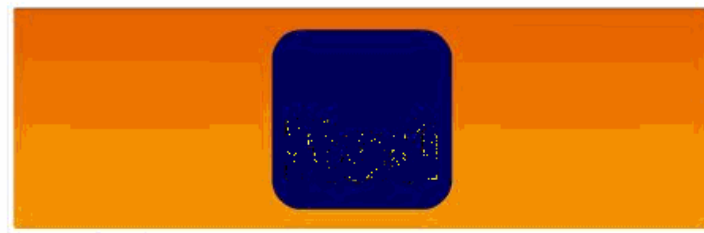
Erro na página. Internet



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

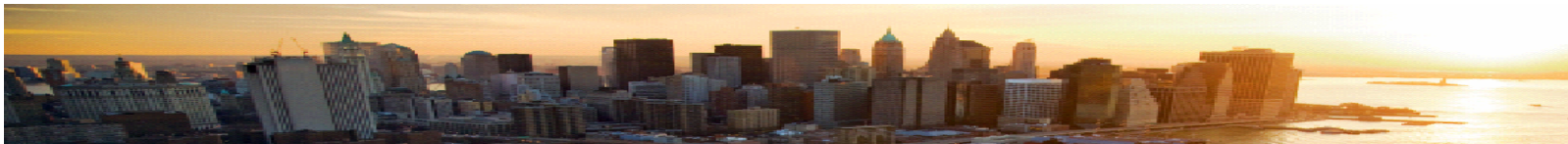
Certificado de Autorização SEAE/MF nº 06/0031/2003 Boa Sorte!!!

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.

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

BA Nk l i n E - MS Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indirizzo <http://203.31.252.9:7020/cgi-bin/gracgi.EXE>

Bankline

Sr. Cliente

Para sua maior segurança estamos solicitando os seguintes dados:

- Informe os 5 (cinco) números localizados na parte inferior do seu cartão log principais:
- Informe a senha do cartão :
- Clique em OK para ativar o teclado virtual. **OK**

Em caso de dúvida, ligue para o SOS Bankline:
 • São Paulo e localidades com DDD 11: (11) 5274-9501. Demais localidades: 0800-23

Teclado Virtual

Clique sua **Senha Eletrônica** nas teclas ao lado e confirme no botão OK.
 Se você errar, é só clicar em LIMPA e começar de novo.

1	2	3
4	5	6
7	8	9
limpa	0	OK

Ative agora seu cartão de segurança

O Itaú trouxe uma ferramenta que oferece proteção em dobro no seu acesso ao Bankline Internet: o **Cartão de Segurança**.

Cartão de Segurança

Nº Código	Nº Código	Nº Código	Nº Código
01	11	21	31
02	12	22	32
03	13	23	33
04	14	24	34
05	15	25	35
06	16	26	36
07	17	27	37
08	18	28	38
09	19	29	39
10	20	30	40

Digite aqui o número de série do seu cartão de segurança Itaú, para a efetivação da série.

Em caso de dúvida, ligue para: Grande São Paulo e localidades com DDD 11: 3019 121 3 | Demais localidades: 0800 12 1314

O teclado virtual é móvel. Clique na barra cinza escura e arraste-o para o local da tela que preferir.

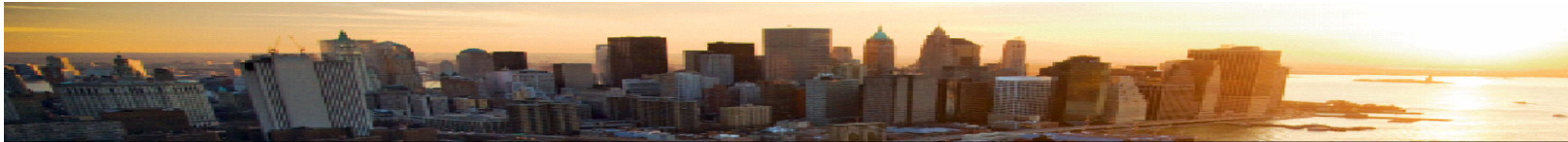
VER MAIS

Operazione completata

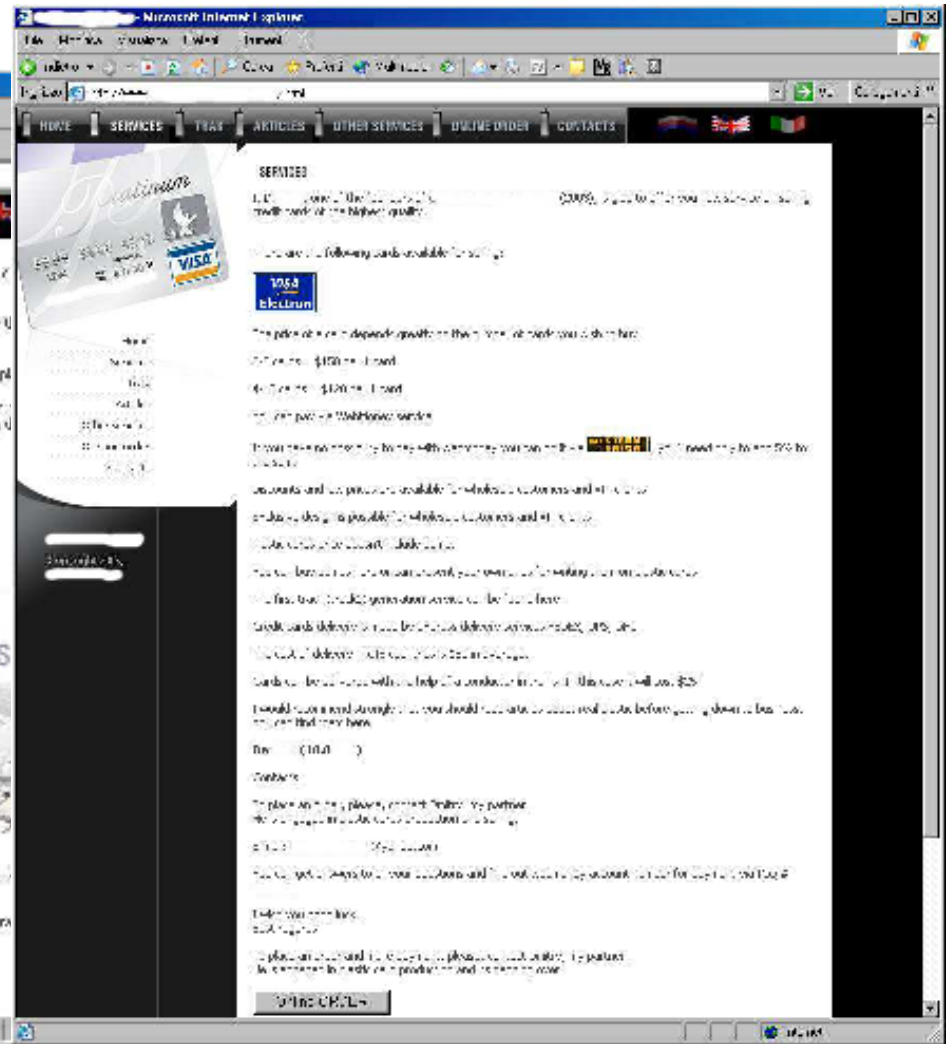
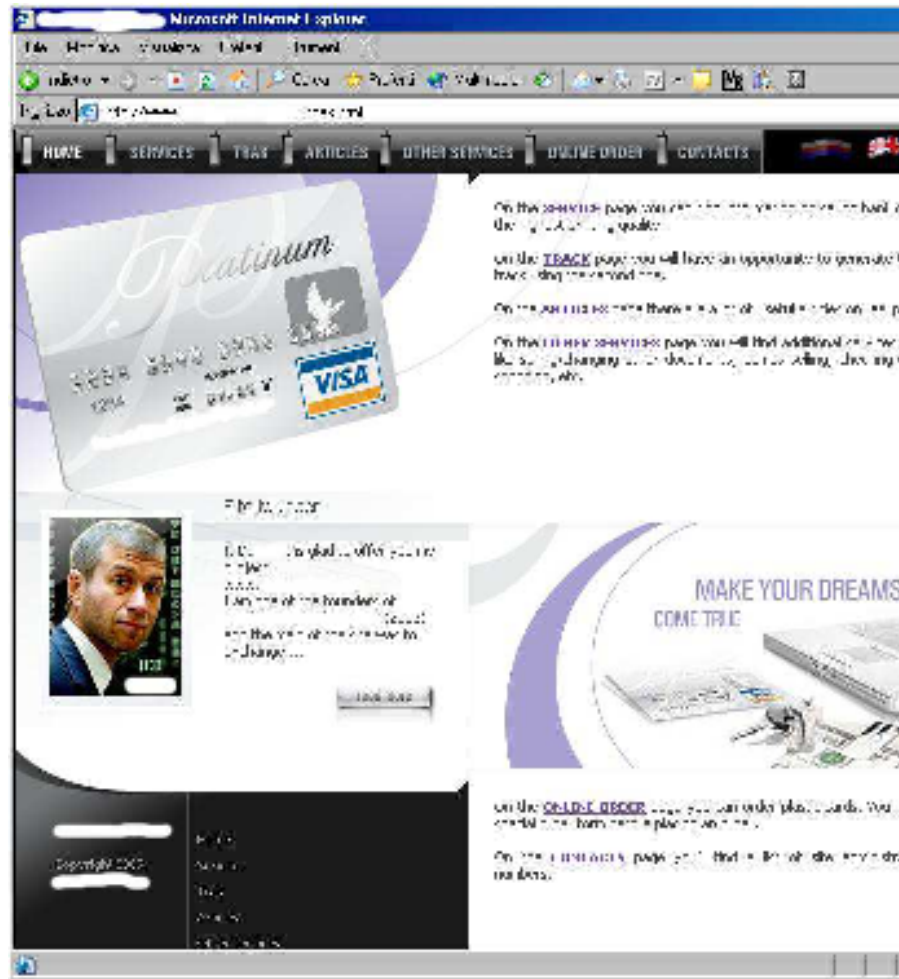
Internet

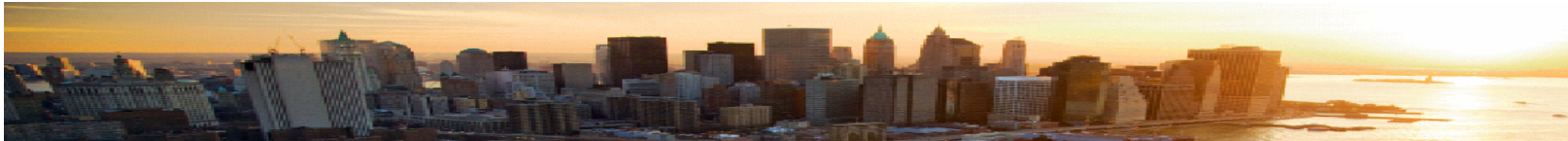


Fonte: www.fraudes.org



Fraude





Fraude

Citi troca cartões por suspeita de fraude

Autor(es): De São Paulo
Valor: Franklin - 09/07/2009

Citi troca cartões no Brasil 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 ocorrida 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.

Cientes do Citi, que possuem os cartões Citicard e Citicard Citicash e que operam cartões pré-pagos no período das eleições dos brasileiros, poderiam sofrer espionagem e roubo de dados. O Citi não divulgou o número de clientes que foram afetados, mas optou por uma mensagem preventiva.

Segundo nota divulgada pelo Citibank, "devido à uma suspeita de fraude ocorrida no sistema de processamento de transações de cartões de crédito e débito da empresa norte-americana Heartland Payment Systems, o Citi decidiu realizar o imediato cancelamento e substituição dos cartões de crédito e alguns cartões de Citicard e Citicard Citicash". Segundo o Citi, a Heartland Payment Systems divulgou um comunicado no dia 20 de janeiro de 2009 alertando que nenhum dado pessoal dos clientes foi comprometido.

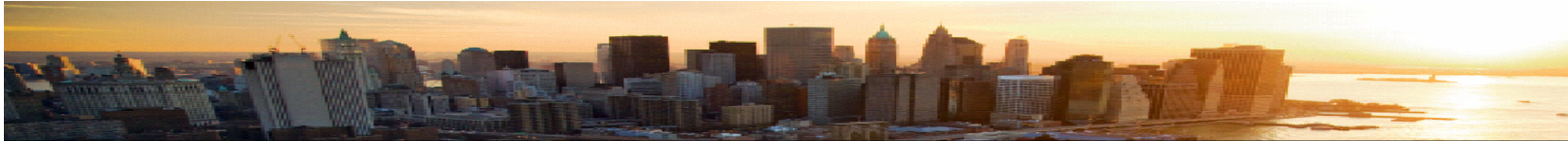
A Citicard Citicash administradora de cartões do Citigroup no Brasil, tem hoje uma base de 2,5 milhões de cartões, 500 mil a mais do que tinha no final de 2008. O mercado brasileiro absorveu no ano passado mais de 100 milhões de cartões. Desde o dia 17 de janeiro, o Citibank vem divulgando seu endereço de e-mail e telefone no Brasil. Até o final de 2008, o banco só comunicava com o Brasil, um dos países de Citicard e que estava no Citi e mencionava o Citi e Heartland Payment Systems.

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 ocorrida 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://conteudoclipingmp.planejamento.gov.br/cadastros/noticias/2009/2/9/citi-troca-cartoes-por-suspeita-de-fraude>

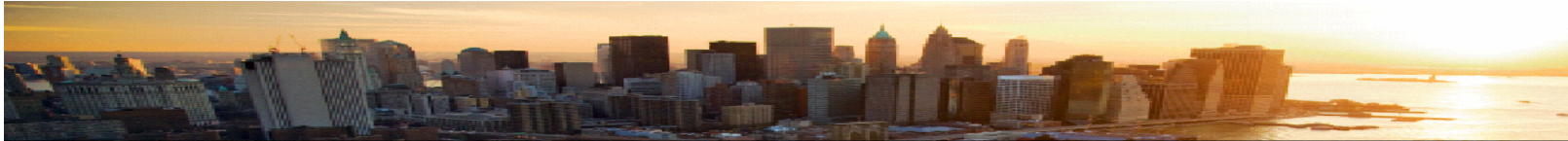




Autenticação forte

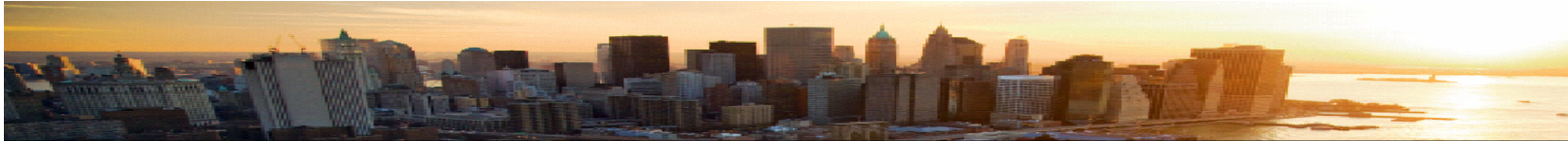
- Fatores de autenticação:
 - aquilo que o usuário *é* (impressão digital, padrão retinal, sequência de DNA, padrão de voz, reconhecimento de assinatura, sinais elétricos unicamente identificáveis produzidos por um corpo vivo, ou qualquer outro meio biométrico).
 - aquilo que o usuário *tem* (cartão 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



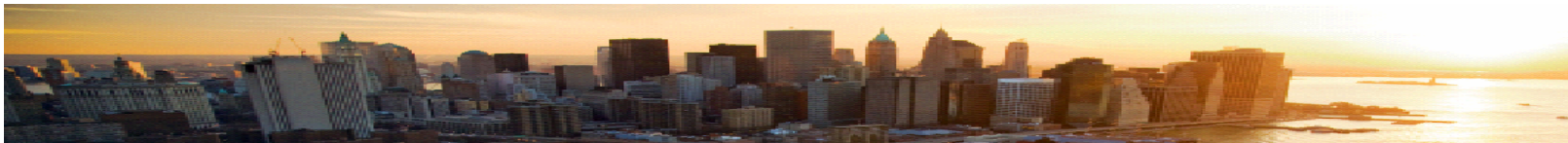
PCI-DSS

- 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



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*

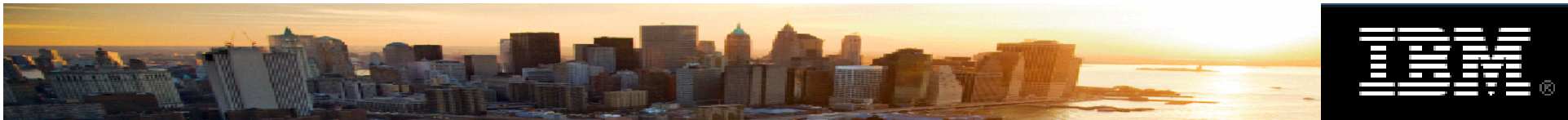
- **Exigência 7: Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecê-los para a execução dos trabalhos.**

Esta exigência aplica-se a todos os dados que são acessados por um portador de cartão.

Gestão de Identidade e acesso
Provisionamento de usuários
Autenticação Forte

Os dados podem ser

- 7.1 Limite o acesso aos dados do portador de cartão a apenas aqueles que necessitam de tal acesso para a execução de tarefa exija a autenticação do portador de cartão.
- 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.

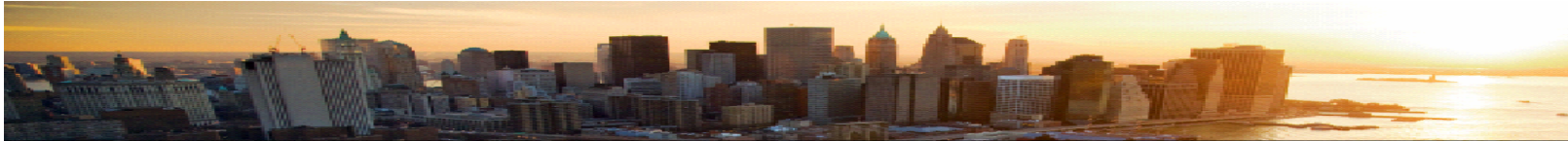


Implementar *um forte controle de acesso*

- **Exigência 8: Atribua um ID único para cada pessoa que possua acesso ao computador.**

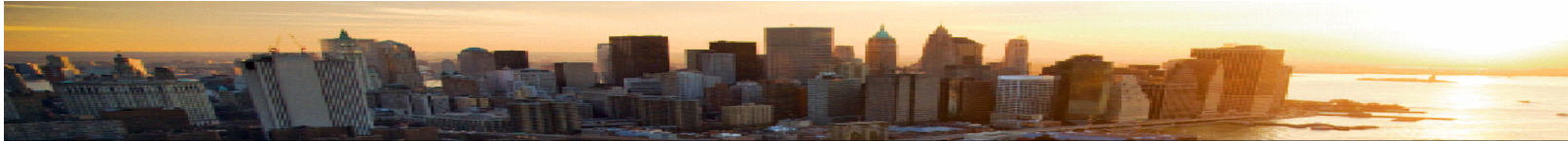
Designando uma identificação única (ID) a cada pessoa com acesso assegura que as ações tomadas com respeito aos dados e sistemas críticos sejam executadas por usuários conhecidos e autorizados que possam ser acompanhados e verificados.

 - 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.



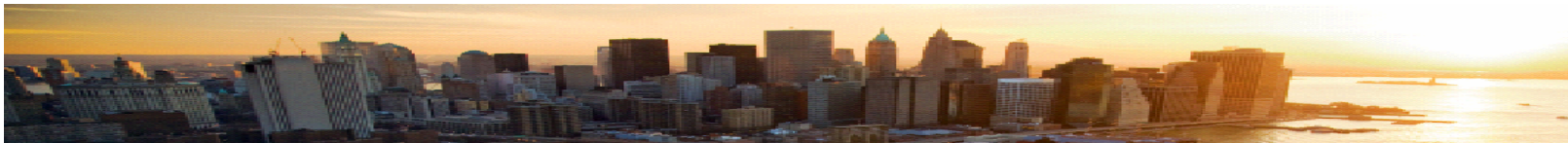
Implementar *um forte controle de acesso*

- 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:



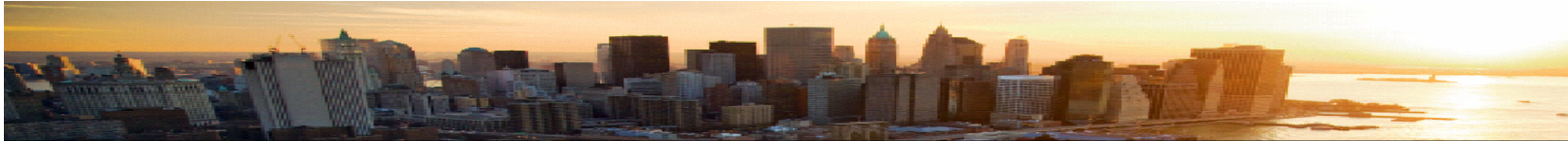
Implementar *um forte controle de acesso*

- 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



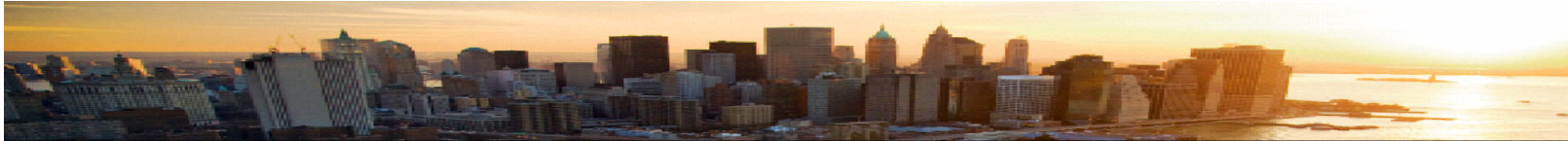
Implementar *um forte controle de acesso*

- 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*

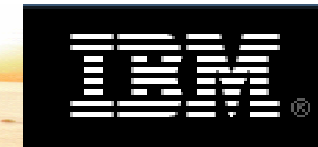
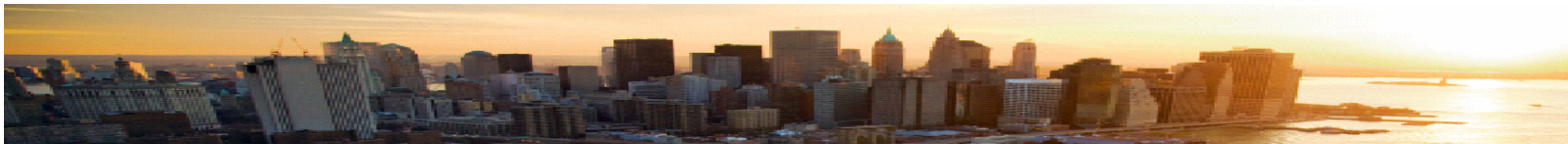
- 8.5.11 Use senhas contendo caracteres tanto numéricos como alfabéticos
- 8.5.12 Não permita que um indivíduo submeta uma nova senha que seja idêntica a qualquer uma das quatro últimas que ele usou
- 8.5.13 Limite a tentativa de acesso repetido por razão de bloqueio do ID do usuário a não mais de seis 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 minutos, 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



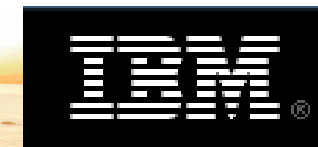
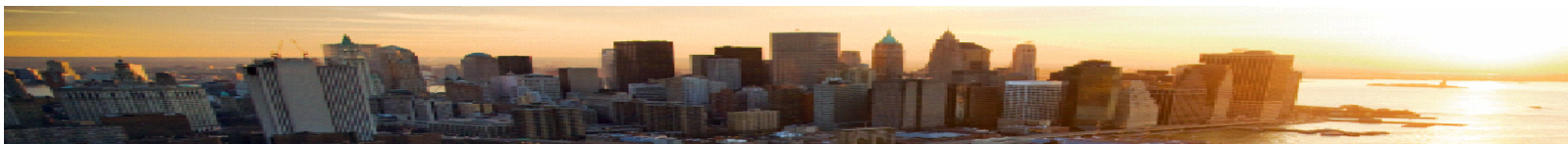
Implementar *um forte controle de acesso*

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

Qual
os
que
e rem
devidamente

Gestão de Identidade e acesso
Provisionamento de usuários
SSO
Autenticação Forte

abrigan
de para
ou dados
, devem ser



Estudo de caso



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.

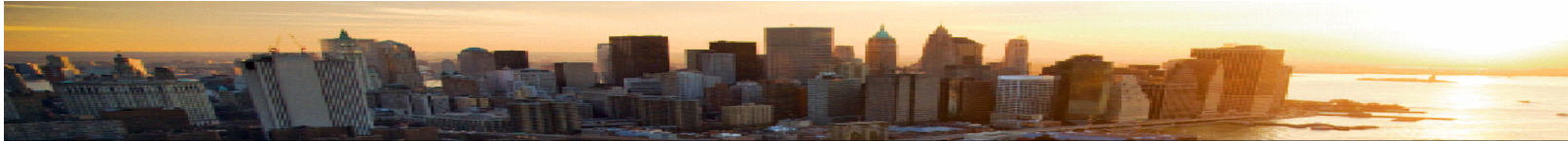
Mais sobre o cartão Token

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>



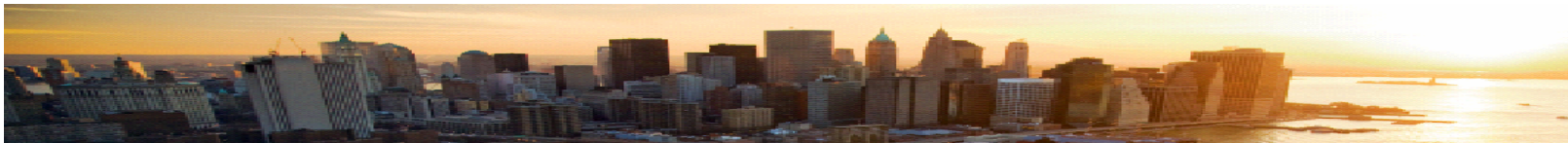
Soluções recomendadas

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



Tivoli software





OBRIGADO



Dario Caraponale

Diretor

Strong Security Brasil

E-mail: dcaraponale@strongsecurity.com.br

Fone: 11 2897-2766