

SEGURANÇA EM TI

Tiago Alves de Oliveira

toliveira@divinopolisuemg.com.br

Segurança da informação

- O que é informação?
Ativo que tem valor para a organização;
É o bem ativo mais valioso da organização?
- Onde está a informação?
Papel;
Banco de dados...
- Por que proporcionar segurança para a informação?

Segurança da informação

- Características básicas da segurança da informação:

Confidencialidade

- A informação é acessada somente por pessoas autorizadas?

Integridade

- Há garantia de que a informação acessada não foi alterada?

Disponibilidade

- A informação está acessível no momento necessário?

Segurança da Informação

- Áreas da segurança da informação:

Segurança física

Segurança lógica

Segurança de pessoas

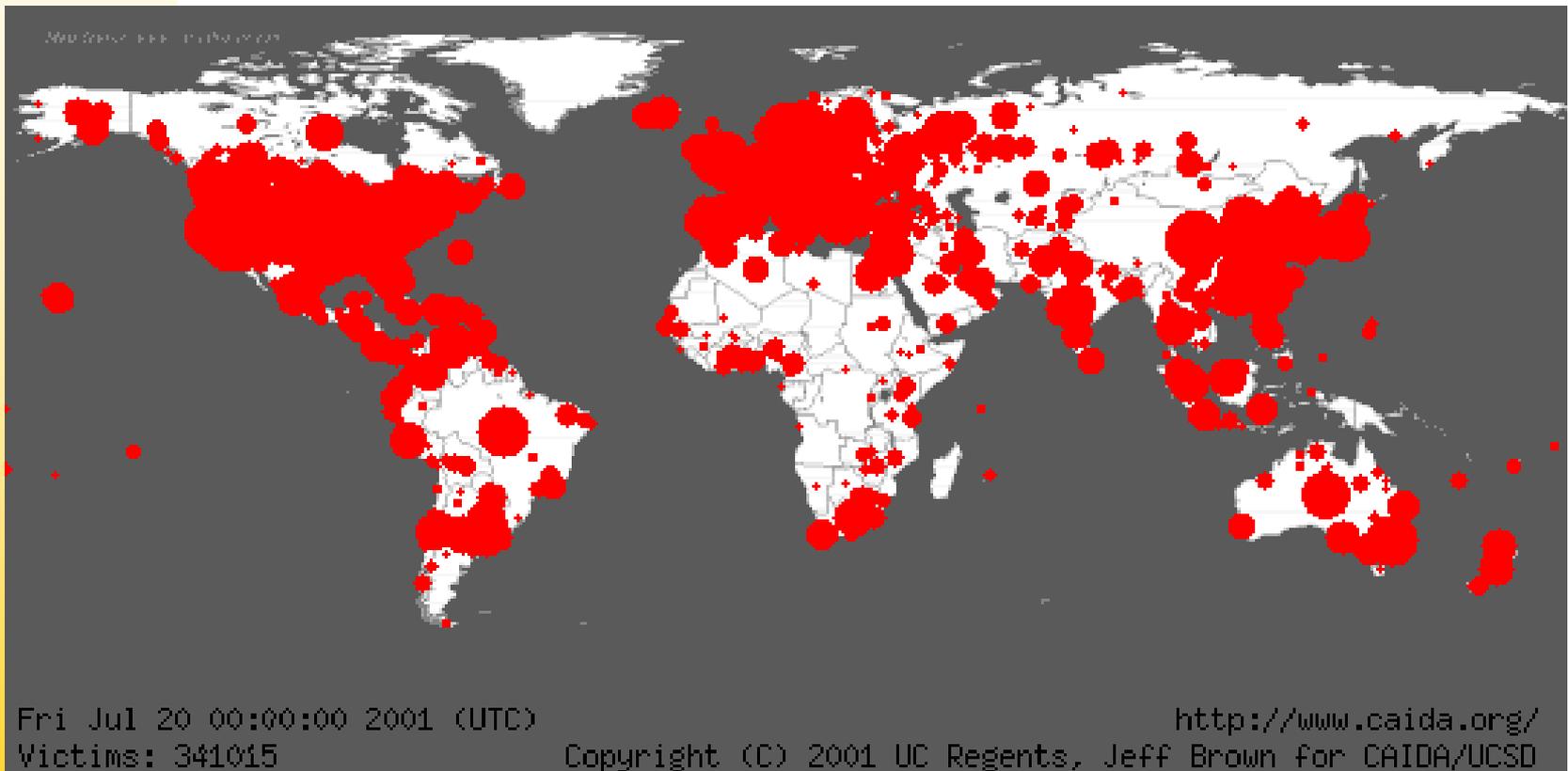
Segurança de computadores

Segurança de redes

Segurança de aplicativos

Ano de 2001

■ *Worm Code Red*



■ Expansão do *worm* Code Red em 14 horas
Fonte: http://www.caida.org/research/security/code-red/coderedv2_analysis.xml

Princípios básicos de segurança

1) Menor privilégio (least privilege)

Princípio fundamental. Define que cada objeto (usuário, administrador, programa...) deve possuir apenas o mínimo de privilégio

2) Defesa em profundidade (defense in depth)

Não se deve confiar em um único mecanismo de segurança; deve-se sempre utilizar defesas redundantes

3) Gargalo (choke point)

Obriga intrusos a usar um canal estreito que pode ser monitorado e controlado

Princípios básicos de segurança

4) Falha segura (fail-safe stance)

Quando o sistema de segurança falha, deve falhar de tal forma que bloqueie o acesso de um invasor, em vez de deixá-lo entrar

5) Participação universal (universal participation)

O sistema de segurança deve envolver todos os objetos (pessoas)

6) Diversidade de defesa (diversity of defense)

Não é um princípio geral. Afirma que o uso de sistemas diferentes torna o sistema (como um todo) mais seguro

Segurança física

- Segurança externa e de entrada
- Segurança da sala de equipamentos
- Segurança dos equipamentos
- Redundância
- Segurança no fornecimento de energia
- Salvaguarda (*backup*)
- Descarte da Informação

Segurança física

- Em nível físico: formação de perímetros e aplicação de três princípios básicos de segurança: defesa em profundidade, gargalo e diversidade de defesa.

1° Terreno: muro, controle de acesso: guarita, seguranças

2° Prédio: paredes, controle de acesso: recepção, seguranças, catracas

3° Callcenter: 2 portas de vidro, controle de acesso: crachá, segurança

4° Datacenter: 2 portas de aço, controle de acesso: crachá+biometria

5° Racks com chave, câmeras



6° Sala cofre

Biometria

- Impressão Digital (Identix TouchSafe Personal)
- Reconhecimento Facial (Miros TrueFace)
- Reconhecimento de Voz (VeriVoice)
- Identificação da Iris (IrisScan)
- Identificação de Retina
- Reconhecimento da Geometria da Mão
- Reconhecimento da Assinatura Manuscrita
- Reconhecimento da Dinâmica de Digitação
- Multi-reconhecimento Biométrico

Segurança física

- Os equipamentos de rede e servidores devem estar em uma sala segura
- Os equipamentos devem ser protegidos contra acessos indevidos no seu console, através de periféricos como teclado, *mouse* e monitor
- Travas para disquetes ou CDs são recomendadas
- Os equipamentos devem ser protegidos contra acessos indevidos ao interior da máquina
- Notebooks ?



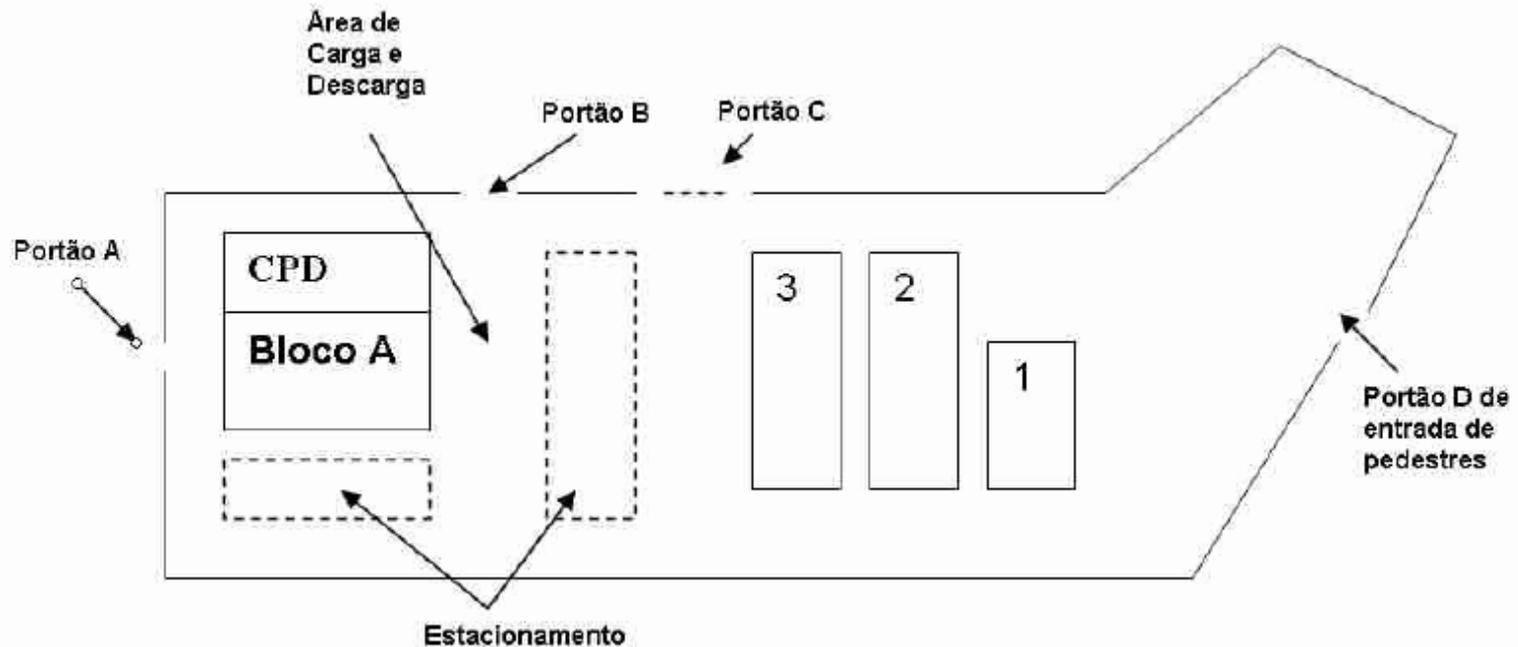
Gabinete de computador com porta e chave



Tranca para gabinete de computador

Principal

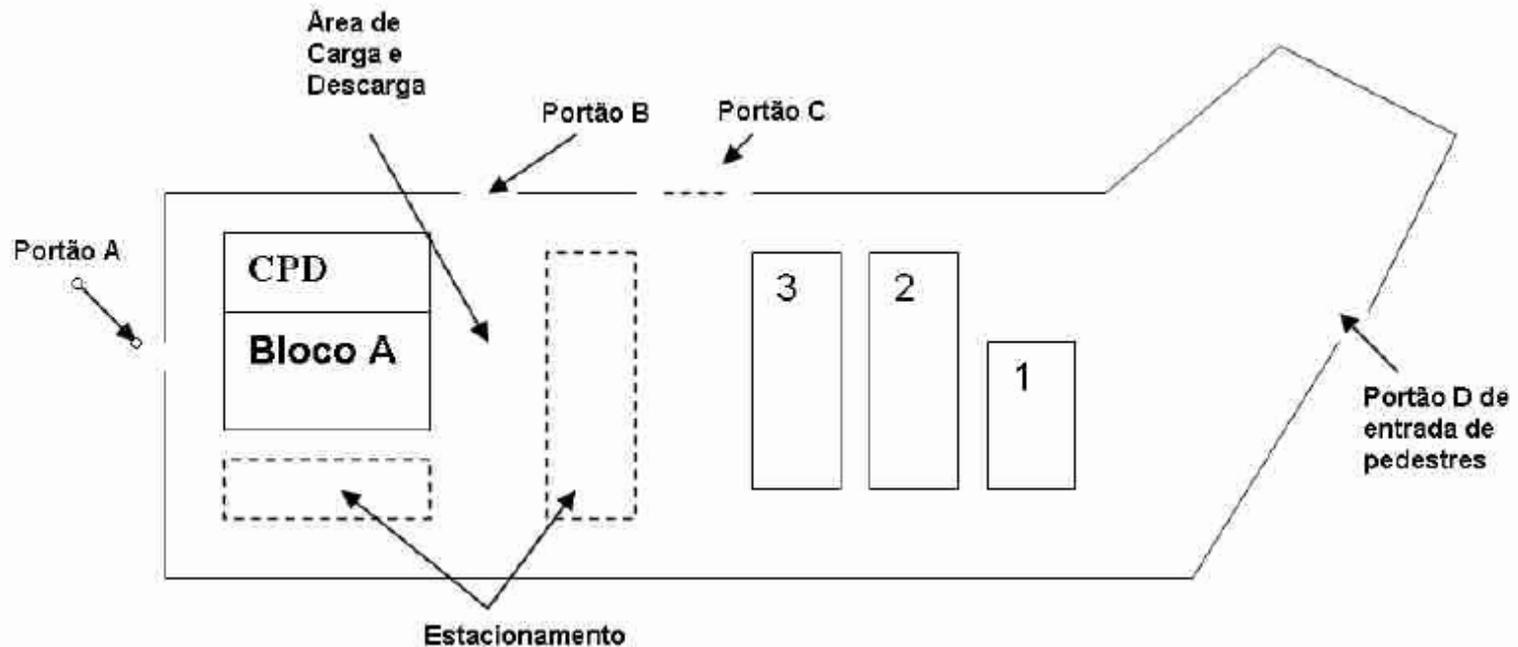
Estudo de caso



O desenho acima mostra o site de uma empresa que abrigará um novo CPD. O terreno é cercado por grades (aprox. 2 metros), com 4 portões:

- Portão A: entrada para o bloco A
- Portão B: entrada de funcionários e de caminhões para carga e descarga
- Portão C: atualmente desativado (portão grande)
- Portão D: entrada de pedestres (portão pequeno)

Estudo de caso



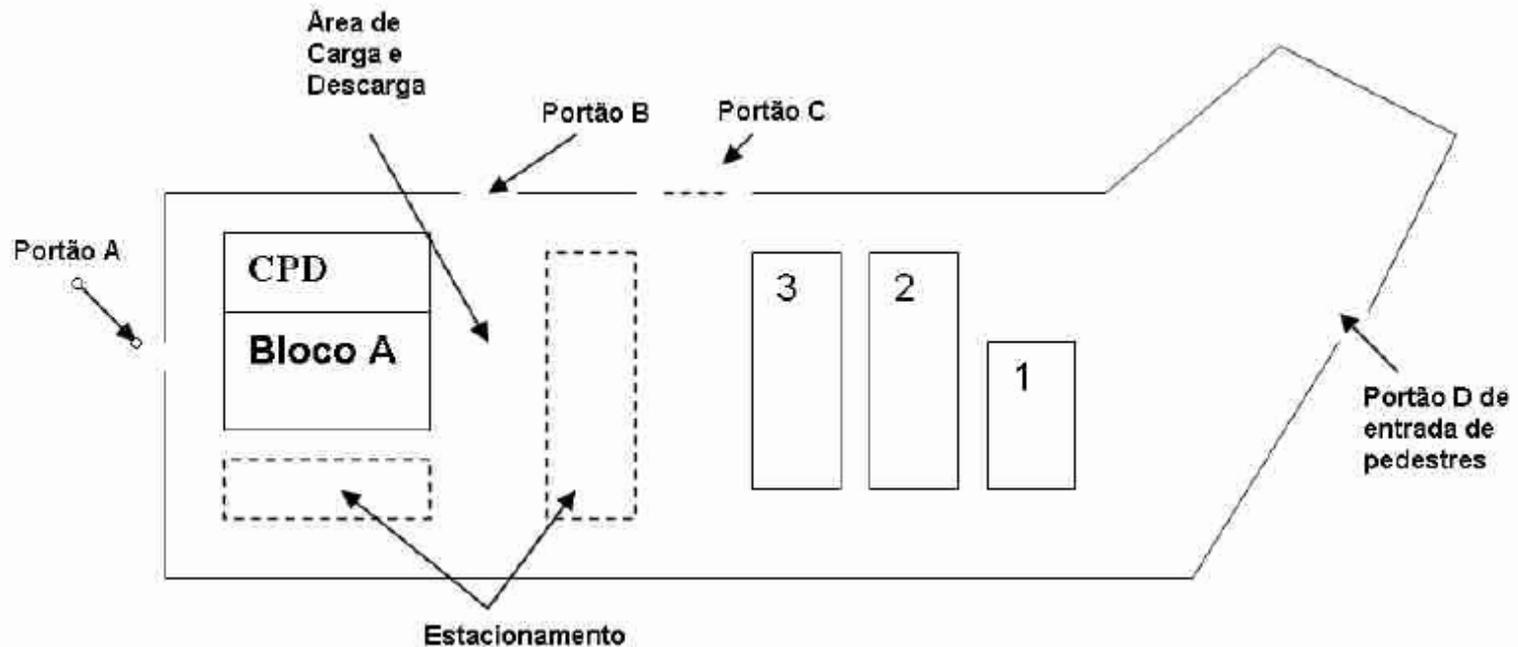
O terreno contém 4 construções:

Bloco A:

No subsolo, há 3 depósitos distintos:

1. papelaria e material de expediente;
2. móveis usados;
3. equipamentos de informática reutilizável.

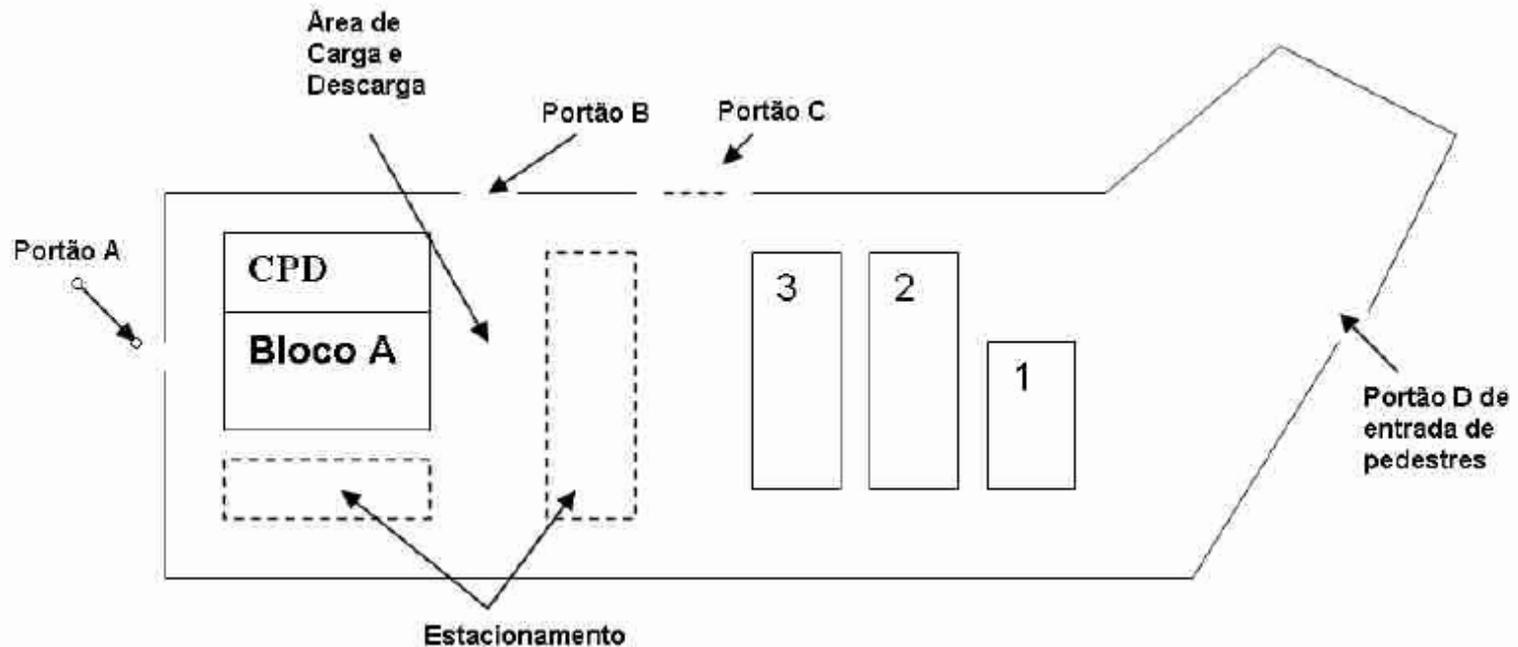
Estudo de caso



No térreo funcionam uma gráfica, um estoque de atacado e a rampa de carga e descarga.

No primeiro andar funcionará o CPD e um novo setor com um grande volume de cheques. Separados do CPD por uma parede corta-fogo estarão a gráfica plana, o escritório e o laboratório da gráfica, que contém materiais altamente inflamáveis.

Estudo de caso



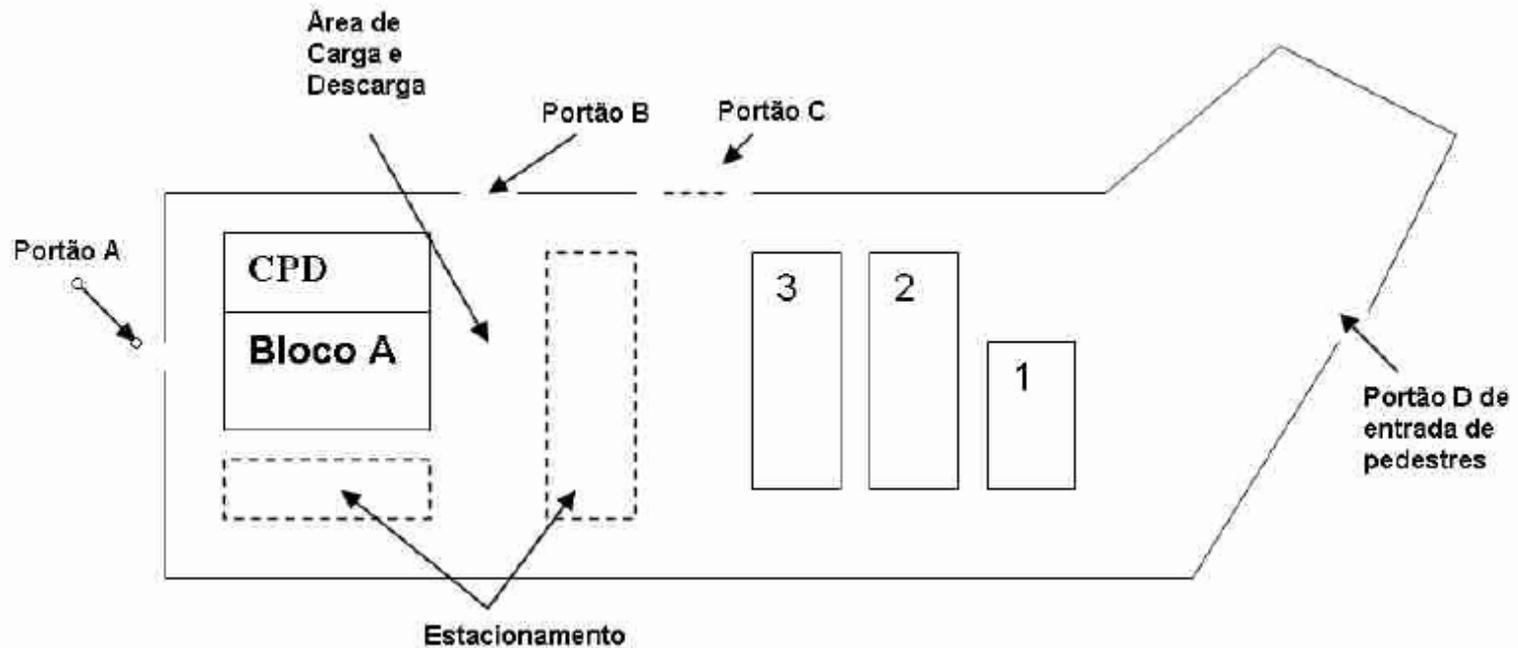
Existem 2 entradas para o CPD. A principal, pelo portão A e uma outra pela área de carga e descarga.

Pavilhão 1: documentos de microfilmagem e papéis

Pavilhão 2: Setorial de transporte, estoque de papel da gráfica e lanchonete

Pavilhão 3: móveis e equipamentos obsoletos

Estudo de caso



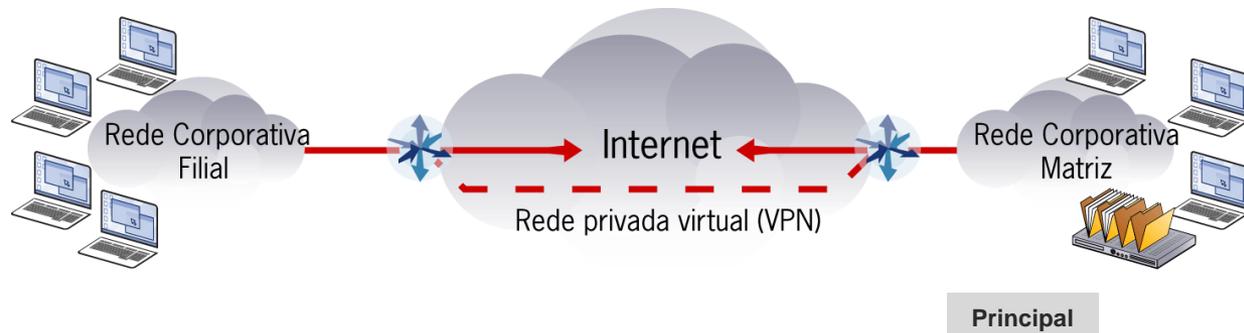
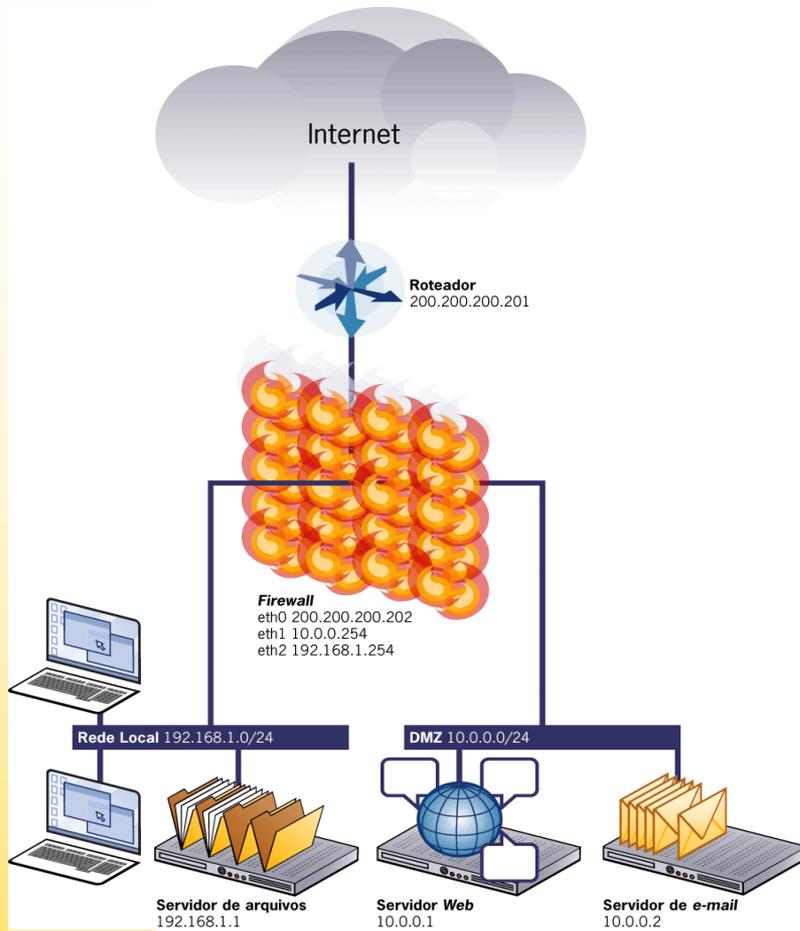
Tendo em vista a segurança física:

1. Quais são os riscos com relação a acesso, incêndio, inundação, etc?
2. Quais ações/soluções vocês recomendariam?

Segurança lógica

- *Firewall*
- Detector de intruso
- Rede virtual privada
- Autenticação, autorização e auditoria

Segurança lógica



Segurança lógica

- Autenticação:

- Identificação:

- Via algo que você sabe
 - Via algo que você tem
 - Via algo que você é

- Autorização :

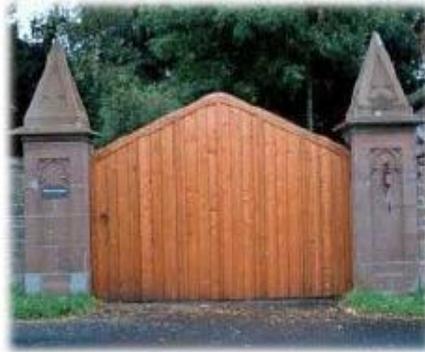
- Perfil

- Auditoria

- Quem fez o quê, quando, aonde?

Morais da Segurança

- As portas dos fundos são tão boas quanto às portas da frente.



Morais da Segurança

- Uma corrente é tão forte quanto o seu elo mais fraco.



Morais da Segurança

- Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.



10 Erros mais Comuns de Segurança

1) A não alteração das senhas de todos os dispositivos da rede.

Problema facilmente resolvido com a troca de senhas "Padrão" por senhas não usuais periodicamente em todos os dispositivos que possuam um *IP*.

2) Compartilhamento de senhas.

Esse péssimo hábito de colocar a mesma senha para vários dispositivos. Isso deve ser alterado por meio de um processo que garanta que as senhas não sejam compartilhadas e sejam trocadas regularmente.

3) Falha no SQL.

Quase 80% dos ataques são por meio da inserção de um código *SQL* em formulários *Web* para atingir banco de dados com essa linguagem. Para evitar isso basta ativar "*firewall*" que filtram as entradas dos formulários e restringir o acesso de dispositivos que não sejam essenciais aos servidores. Assim a empresa previne o acesso através de um erro de *SQL*.

10 Erros mais Comuns de Segurança

- 4) **Configuração na lista de controle de Acesso, má revisada ou autorizada.**

Para simplificar ainda mais a solução desse problema é segmentar a rede com uma lista de controle de acesso. Mais cuidado, caso o *hacker* consiga entrar na rede de um dos seus parceiros e seu servidor não tiver adequadamente protegido, seus dados estarão disponíveis.

- 5) **Uso de acesso remoto ou *softwares* de gerenciamento sem segurança.**

Programas como o VNC são caminhos de entrada de *hackers*. E a única forma é o profissional fazer uma varredura externa de todo o endereço IP procurando por tráfego desse tipo de *software*. Encontrando, deve-se tomar medidas extras de segurança, como certificados que se juntem as senhas.

- 6) **Busca de vulnerabilidade básica em aplicações não-críticas.** Para garantir testes devem ser feitos em todas as aplicações abrangendo pelo menos as vulnerabilidades básicas, mais lembre-se o *hacker* não escolhe o ataque pelas aplicações críticas mais pela ordem do que é mais fácil.

10 Erros mais Comuns de Segurança

7) Falta de proteção contra *Malwares*.

Malwares instalados nos servidores são responsáveis por cerca de 40% de todas as brechas em segurança. Esse tipo de proteção roda somente em servidores críticos e o ideal é fazer uma varredura em toda a rede.

8) Falha em proibir tráfego externo em roteadores.

Para evitar a infiltração de *Malwares* e o uso dos mesmos por *hackers* basta a aplicação de uma lista de controle de acessos, bloqueando assim o servidor de enviar dados que não deveria. **ex.** um servidor de e-mails de enviar somente *e-mails* e para sua lista de contatos.

10 Erros mais Comuns de Segurança

9) Falta de conhecimento de onde dados críticos estão armazenados.

A maioria das Empresas acreditam saber onde estão os dados como CPFs, cartões de crédito, adotando o nível mais alto nesses servidores, mais se esquecem que em outros departamentos podem existir *backups* e esses são chamados de servidores secundários. Normalmente são esses servidores secundários que vazam os dados.

10) Indústria de pagamentos – Falta de atenção aos padrões de segurança.

A indústria financeira tem várias regras que seguidas com rigor são muito eficazes para garantir a segurança dos pagamentos.

- O que leva uma pessoa a invadir um sistema?

Impunidade

Delinqüência

Tentativa de chamar a atenção

Vingança

Compensação financeira

Espionagem

Ameaças recentes

Fraude *on-line*:

Visa seqüestro de dados bancários e informações úteis ao malfeitor

Aborda em larga escala usuários via *e-mail*

Usa assunto atrativos como disfarce

Induz a vítima a fornecer dados sigilosos

Instala programa que rouba informações no computador

Phishing Scam

Formas atuais

Link para programa malicioso

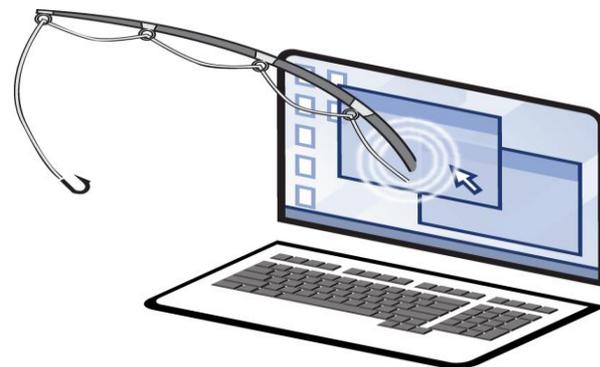
Página falsificada de comércio eletrônico ou *internet banking*

E-mail contendo formulário

Mensagens Maliciosas

Cuidados ao usar comércio eletrônico ou *internet banking*

Proteção anti-*phishing*



Phishing Scam

http://forms.visualnetworks.com/forms/indexIE.html

Itaú Bankline AGÊNCIA CONTA

Itaú

Conheça o Itaú | Conta Corrente | Investimentos | Vida e Previdência | Cartões de Crédito | Empréstimos | Seguros | Acesso Internet

Digite os números que constam no seu cartão conforme exemplo ao lado.



Agência:

Conta:

Senha Eletrônica:

Senha do Cartão:

5 Dígitos do Cartão:

Data de Nascimento:

Número do Portador:

Dicas de Segurança

No acesso ao Itaú Bankline, confira seu nome antes de digitar sua senha eletrônica.

SUPERNOVAS

Cliente apresenta cliente
Participe da promoção e ganhe prêmios.

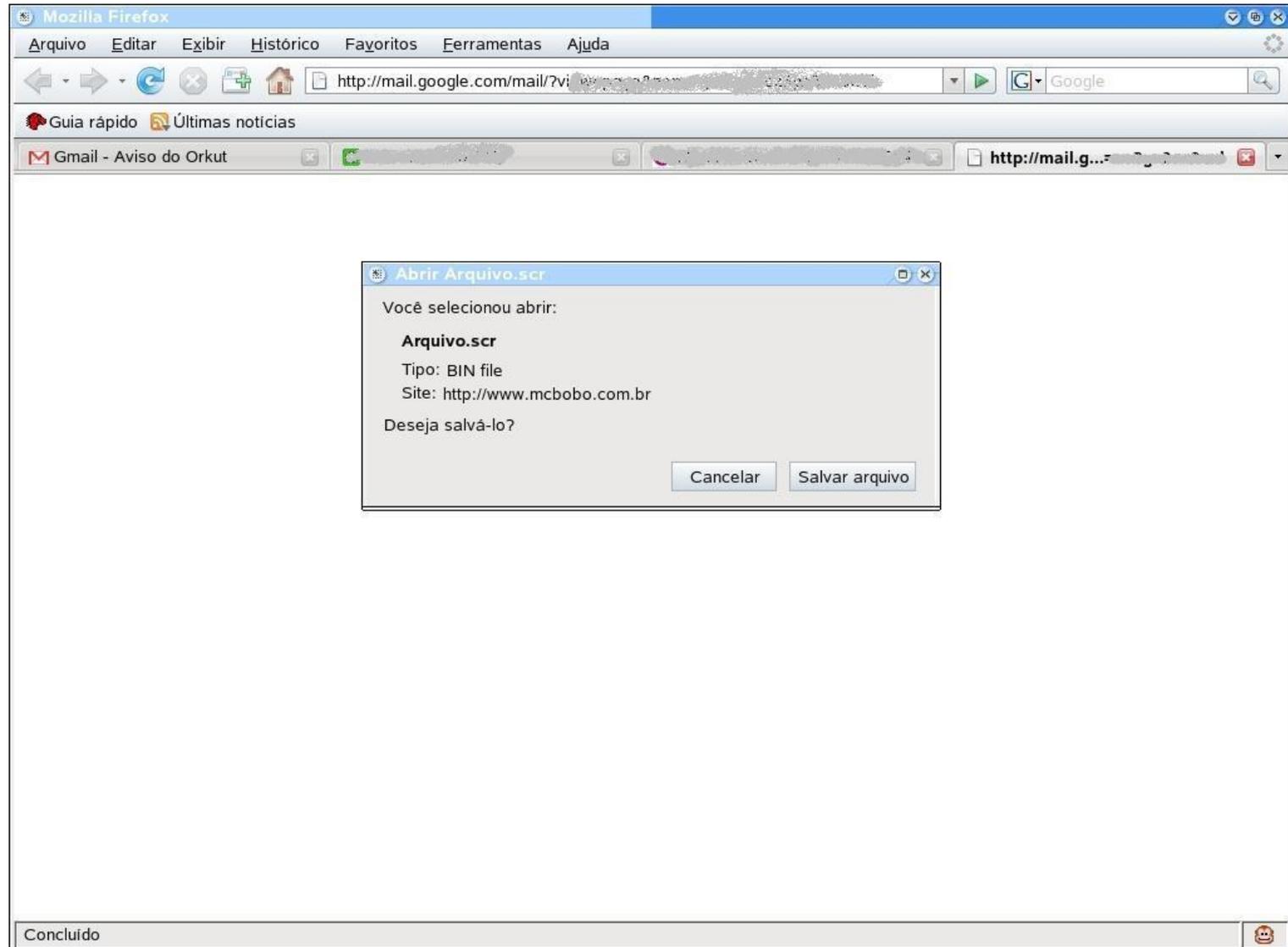
Travellers Cheques Itaú
Muita facilidade e segurança. Conheça as vantagens.

É dia de ganhar com Itaúcard.
Participe desta promoção exclusiva: são 92 prêmios de R\$ 3.000,00, um para cada dia da promoção!

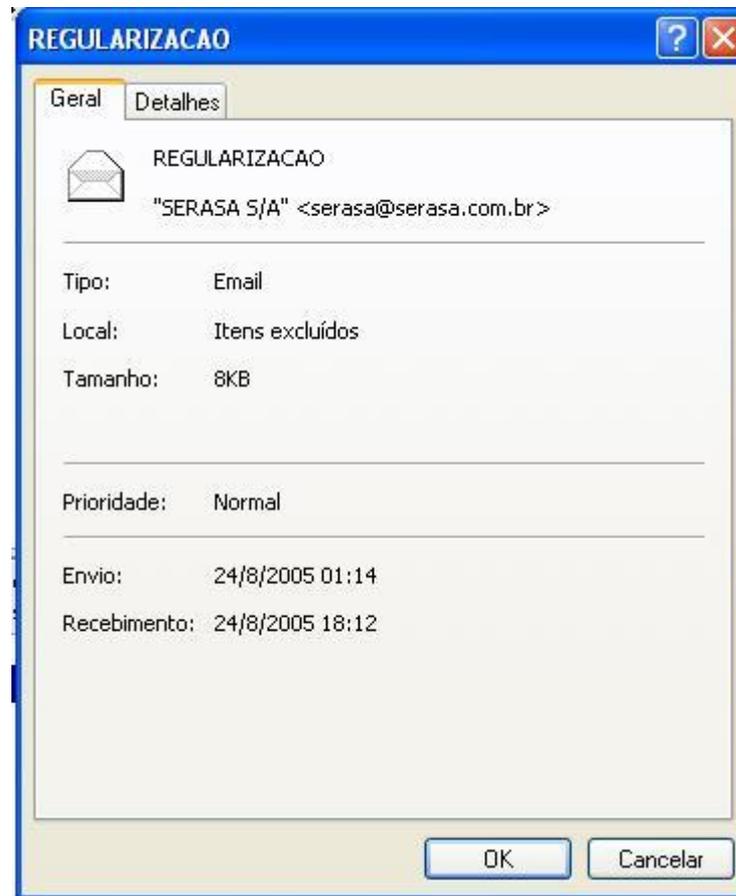
13º
Não deixe para o fim do ano!
Contrate o Credipré 13º e faça agora tudo o que você não pode deixar para depois.

Relações com Investidores | Imprensa | Notícias e Cotações | Itaú Cultural | Itaú Social | Oportunidades de Carreira | Segurança e Privacidade | Fale Conosco

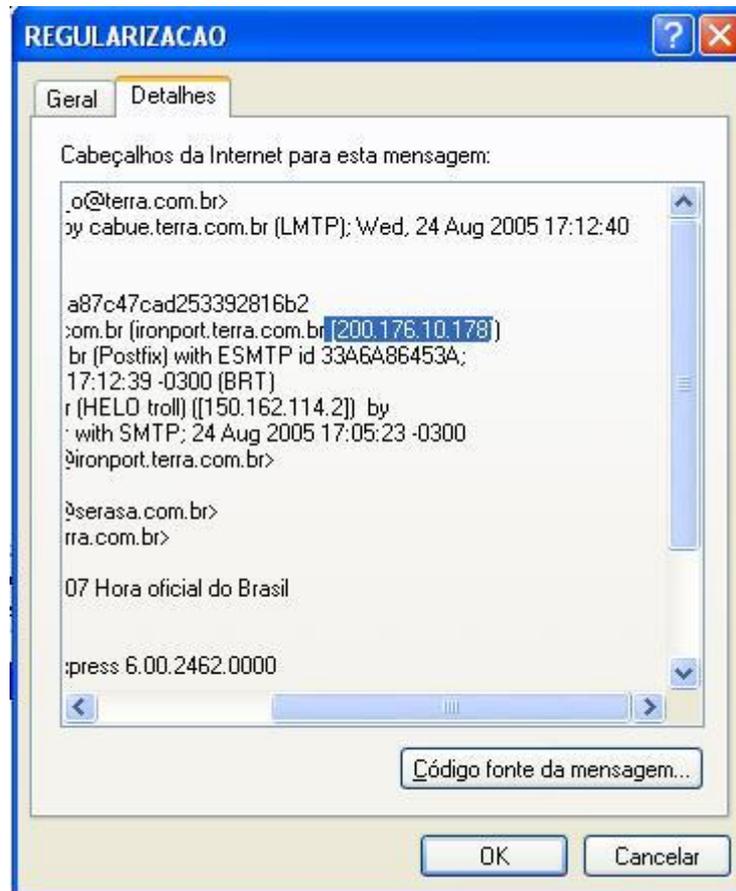
Phishing Scam



Phishing Scam



Phishing Scam



Phishing Scam

The screenshot shows a Mozilla Firefox browser window displaying a phishing email from 'Equipe do Windows Live'. The email header includes the sender 'postmaster@email.com', the date 'domingo, 27 de abril de 2008 13:49:24', and the recipient 'parkcdi@hotmail.com'. The body of the email contains instructions for password recovery, including a list of steps and a URL: <https://accountservices.msn.com/EmailPage.srf?emailid=647f5e5e892e5b19ced=ByRnm14yAzAjM9qSietVt.sdBhU%2BwP5>. A black arrow points to this URL. At the bottom of the browser window, another URL is visible: http://akisalra.t35.com/inferno_E.html, which is circled in red. Large red text 'LINK FALSO' is written across the bottom of the email content, with a red arrow pointing to the circled URL. A yellow warning banner at the top of the email content reads: 'Os anexos, as imagens e os links desta mensagem foram bloqueados para sua segurança. Mostrar conteúdo'.

Windows Live Hotmail - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://by113w.bay113.mail.live.com/mail/ReadMessageLight.aspx? GO Google

Forum Hacke... Postem aqui... Videos Hack... Forum Hacke... 4shared - fr... ME AJUDEM... Precizando C... Windows Liv... Window...

Os anexos, as imagens e os links desta mensagem foram bloqueados para sua segurança. Mostrar conteúdo

Recebemos seu pedido para troca de sua senha

De: **Equipe do Windows Live** (postmaster@email.com)
Você pode não conhecer este remetente. Marcar como confiável | Marcar como não confiável

Enviada: domingo, 27 de abril de 2008 13:49:24
Responder-Para: Equipe do Windows Live (postmaster@email.com)
Para: parkcdi@hotmail.com

Olá, Recebemos sua solicitação para redefinir sua senha do Windows Live.
Para confirmar a solicitação e redefinir a senha, siga as instruções abaixo.
A confirmação da solicitação ajuda a evitar o acesso não autorizado à sua conta.

Se você não solicitou a redefinição da senha possa ser que alguém está tentando entra em sua conta, siga as instruções abaixo para cancelar a solicitação.

1.CONFIRMAR A SOLICITAÇÃO E REDEFINIR A SENHA

<https://accountservices.msn.com/EmailPage.srf?emailid=647f5e5e892e5b19ced=ByRnm14yAzAjM9qSietVt.sdBhU%2BwP5>

Confirma a solicitação conforme descrito acima.

3.Siga as instruções na página da Web que é exibida.

CANCELAR A REDEFINIÇÃO DE SENHA.

<https://accountservices.msn.com/EmailPage.srf?emailid=647f5e5e892e5b19ced=ByRnm14yAzAjM9qSietVt.sdBhU%2BwP5>

3. Siga as instruções na página da Web que é exibida

LINK FALSO

http://akisalra.t35.com/inferno_E.html

1.453s

Iniciar Windows Live Hotmail... Bleach Nicolas - Conversa 17:36

Phishing Scam

The screenshot shows a Gmail interface in a Mozilla Firefox browser. The email subject is "Voce ira explicar seus atos!". The sender is "Polícia Federal <departamento@pf.com.br>". The email body contains a blacked-out header, a logo for "Departamento de Polícia Federal", and a message in Portuguese. The message states that the sender's IP address was logged on an illegal site and that a judicial inquiry will be opened within 48 hours. It includes a link "CLIQUE AQUI" and contact information for Superintendent DPF Daniel Gomes Sampaio. The address is SAIS Quadra 7 - Lote 23 - Setor Policial Sul Brasília-DF, CEP 70610-901, with phone number (0xx-61) 3345-9500. A red arrow points to the "Reply" button at the bottom of the email.

Voce ira explicar seus atos!

from: **Polícia Federal** <departamento@pf.com.br>
to: celso@pf.com.br
date: Aug 28, 2007 8:38 PM
subject: Voce ira explicar seus atos!


 Departamento de Polícia Federal

Senhor/Senhora,

Seu endereço de IP foi logado em um site ilegal. Precisamos que o fato venha a ser esclarecido o mais rápido possível, caso não seja esclarecido em até 48 horas, será aberto inquerito judicial. Entre em contato para esclarecer o fato.

Contato e esclarecimentos do inquérito [CLIQUE AQUI](#)

Esperamos contato o mais rápido possível para devidos esclarecimentos.

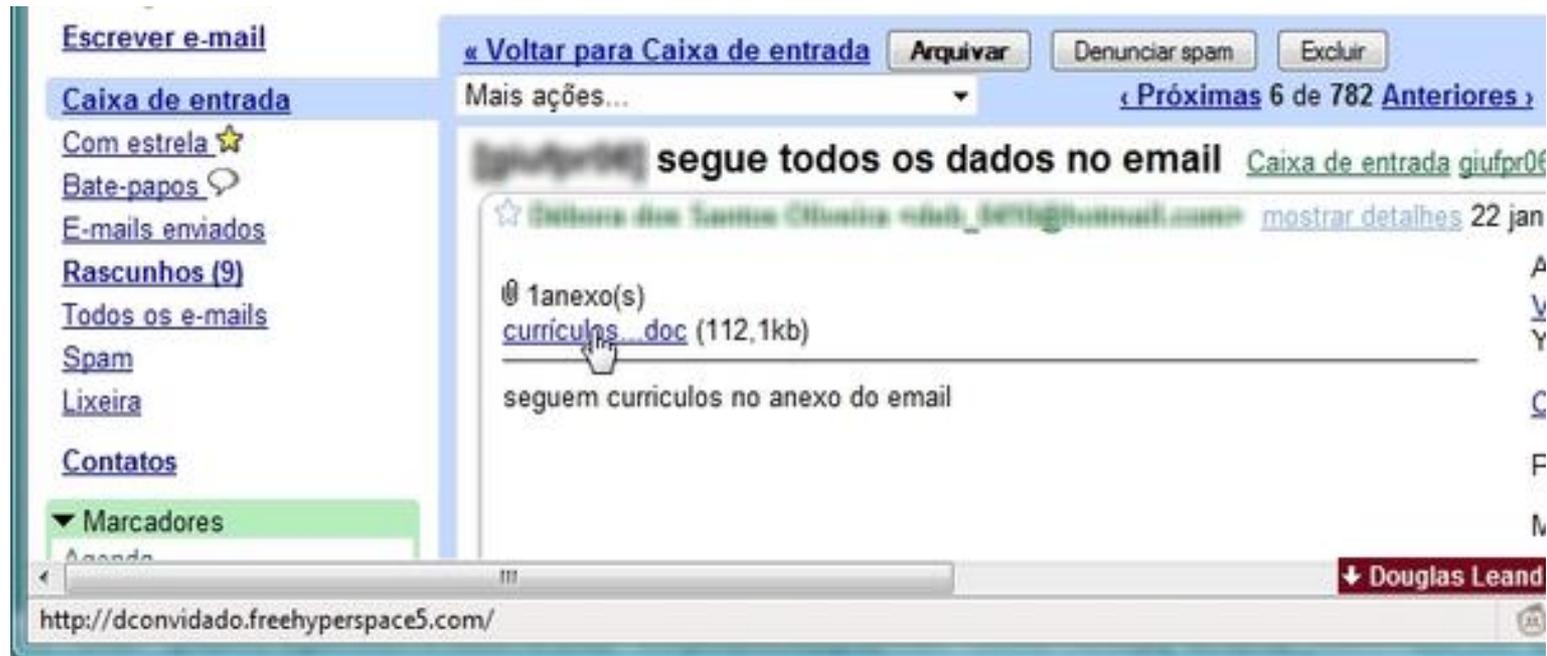
Superintendente:
DPF Daniel Gomes Sampaio

Endereço:
SAIS Quadra 7 - Lote 23 - Setor Policial Sul Brasília-DF
CEP 70610-901
(0xx-61) 3345-9500

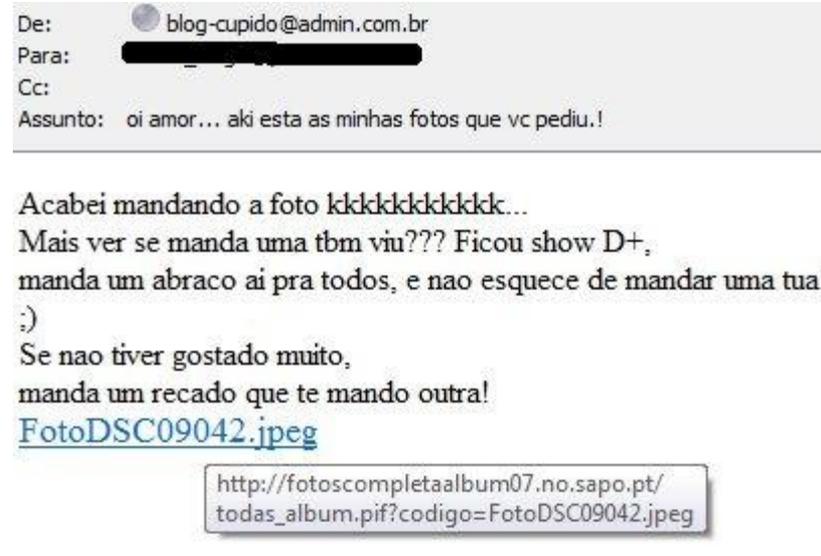
Reply Forward Invite Policia to Gmail

<http://www.minart.org/new/page/www.pf.com>

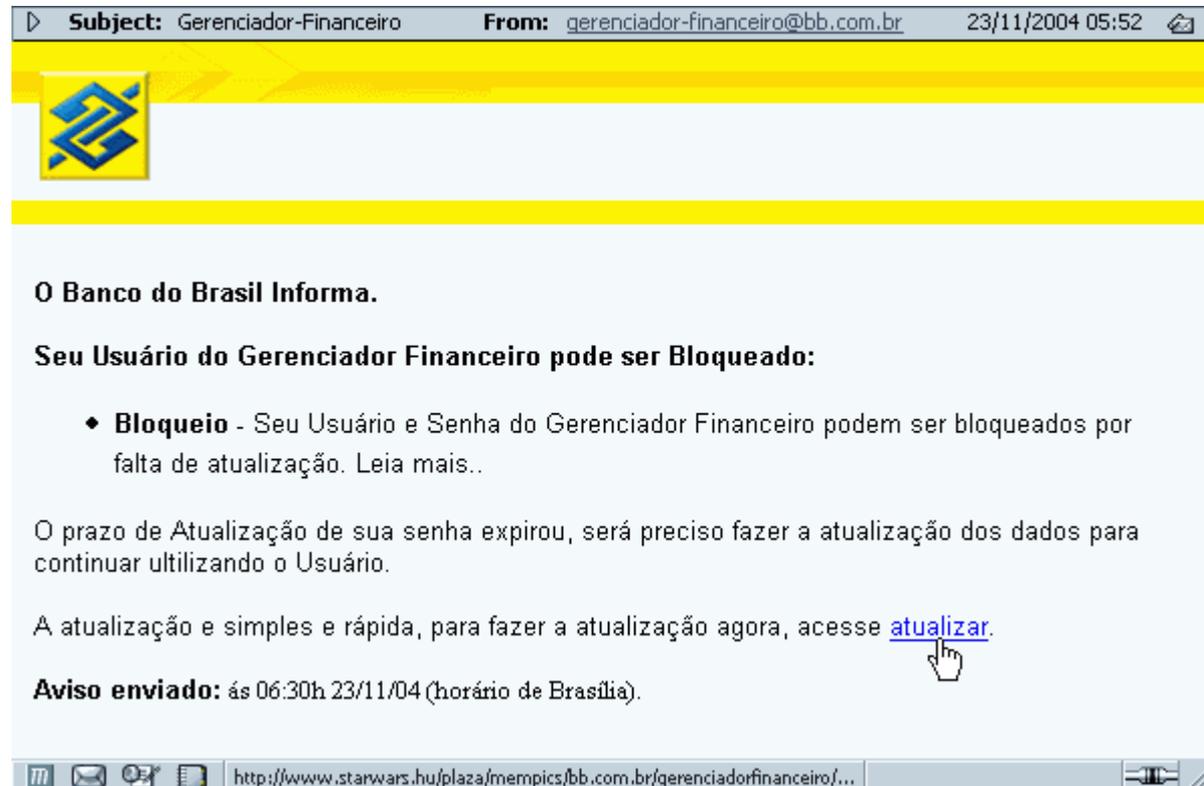
Phishing Scam



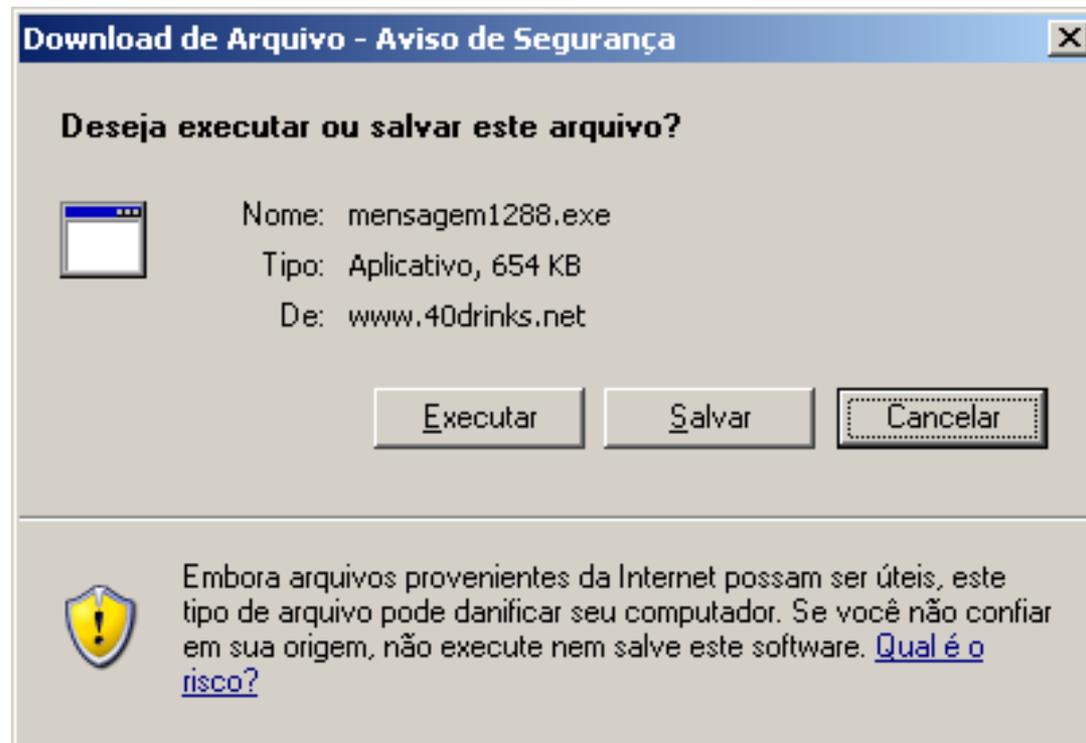
Phishing Scam



Phishing Scam



Phishing Scam



Phishing Scam

Assunto: Alguém que lhe ama acaba de lembrar de você De: [Alguém que lhe ama acaba de lembrar de você](#) 05/08/2006 21:58

ocarteiro.com

Tenho uma novidade para você!



Olá **Meu Amor**, venho te entregar este cartão:
<http://ocarteiro.com.br/lercartao.php?id=59554A46821571> que vai estar disponível por 30 dias.

Ver meu cartão

Você também poderá visualizá-lo em <http://www.ocarteiro.com.br> colocando o número do seu cartão: **1902667279A7383**

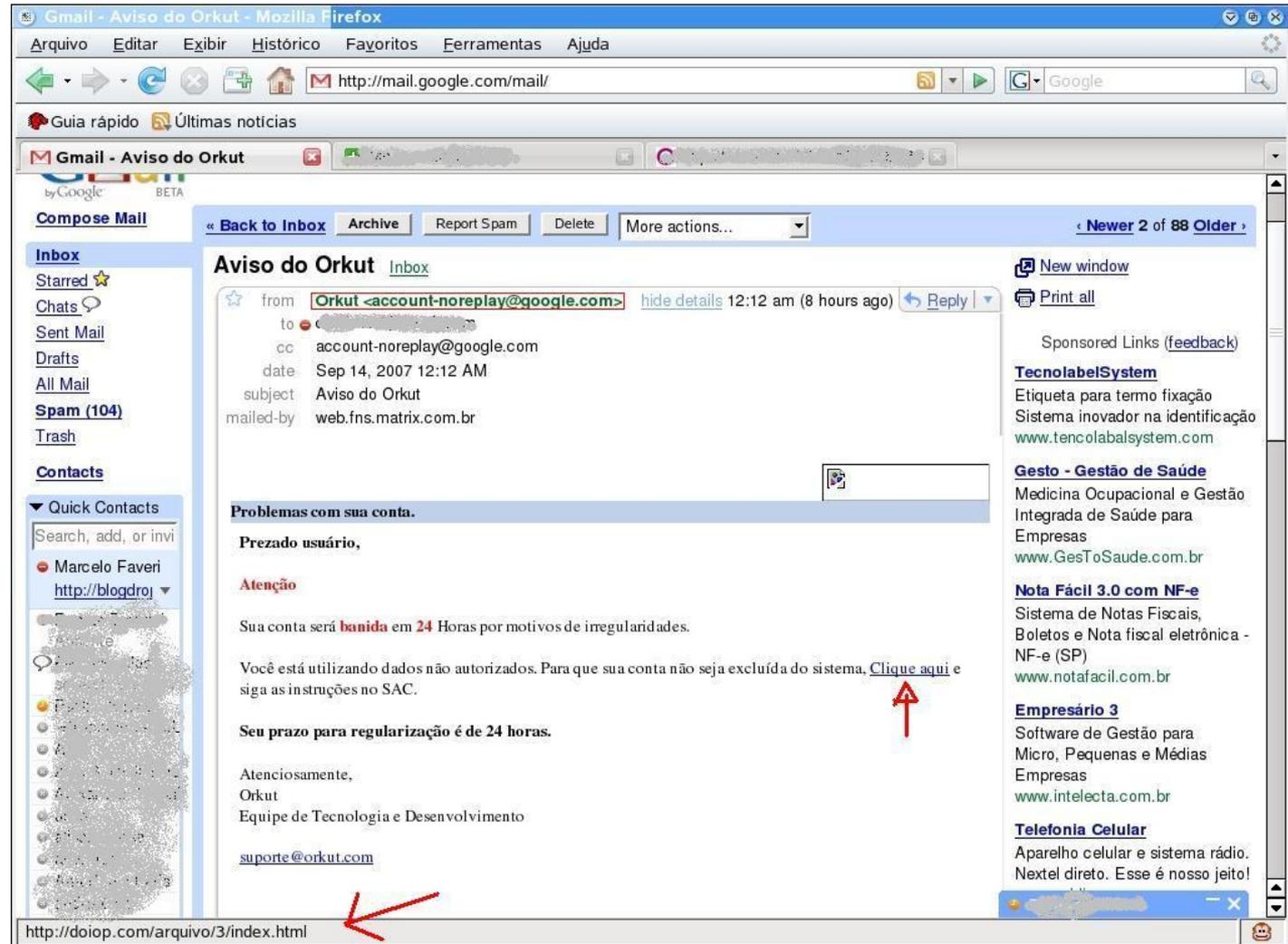
Terei o maior prazer em entregar seus cartões também.
Um abraço,
ocarteiro.com.

PUBLICIDADE:

Proteja seu PC de intrusos, curiosos e invasores  **Protect Me**
Faça o download!

<http://www.40drinks.net/modules/mensagem1288.exe>

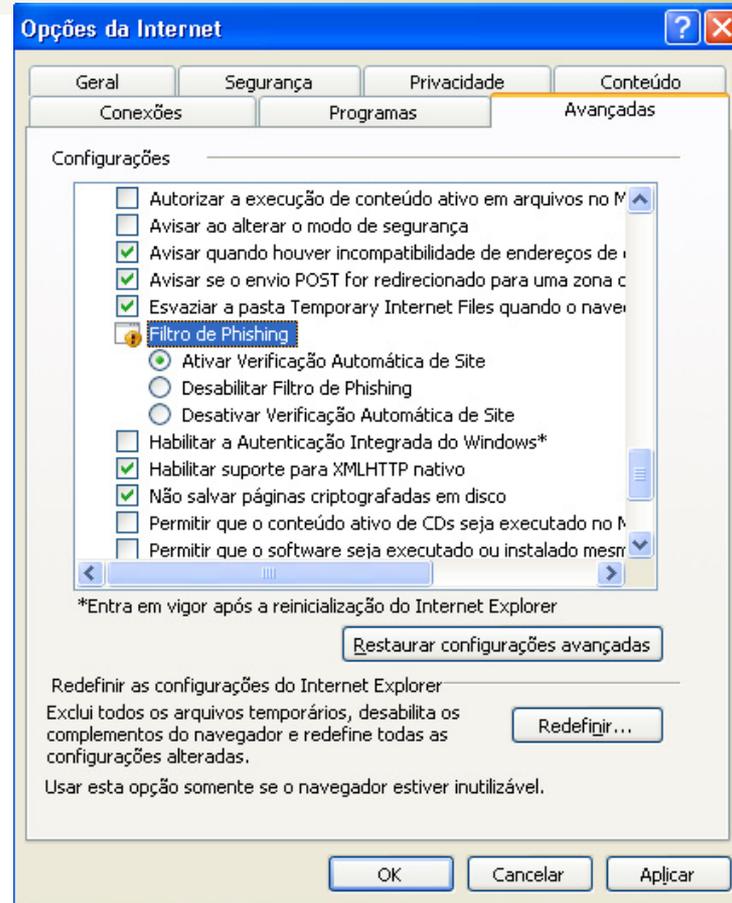
Phishing Scam



Phishing Scam



Phishing Scam



Identificação

- Identificação de todos os ativos de informação importantes

Ativo	Descrição
Hardware	Estações, computadores pessoais, impressoras, roteadores, <i>switches</i> , <i>modems</i> , servidores de terminal e <i>firewalls</i>
Software	Código fonte, programas executáveis, utilitários, programas de diagnóstico, sistemas operacionais e programas de comunicação
Dados	Dados armazenados <i>online</i> e dados arquivados, <i>backups</i> , <i>logs</i> de auditoria, bancos de dados e dado em trânsito em meios de comunicação
Pessoas	Usuários, Administradores e operadores
Documentação	Manuais de programas, <i>hardware</i> interno, sistemas e procedimentos locais de administração

Identificação

- ▲ **Nível de criticidade**
 - Nível de importância dentro da instituição

Ativo	Classificação	Valoração	Criticidade
Correio eletrônico interno	Administrativo	Moderado	Média
Salários dos empregados	Financeiro	Alto	Média
Tendências de mercado	Pesquisa	Baixo	Baixa
Patentes pendentes	Proprietário	Alto	Alta
Balanço anual	Financeiro	Moderado	Alta

Vulnerabilidades e ameaças

▲ Vulnerabilidade

- Evidência ou fragilidade que eleva o grau de exposição do ativo, aumentando a probabilidade de sucesso da investida de uma ameaça
- É preciso conhecer as vulnerabilidades de cada ativo

Vulnerabilidades		
Físicas	Tecnológicas	Humanas
Cabeamento de baixa qualidade	Defeito de software	Falta de conscientização dos usuários
Ausência de fragmentadora de papel	Sistema operacional desatualizado	Ausência de rotinas de backup
Instalação elétrica mal dimensionada	Senha fraca	Descuido e despreparo

- ▶ **Neste cenário temos 50 empregados ociosos:**

8 (horas/dia) x 240 (dias/ano) x 50
(número de pessoas) = 96.000 horas

R\$ 50,00 (custo/hora) x 96.000 (horas) =
R\$ 4.800.000,00

Custo direto (fixo) da empresa com os
50 funcionários durante um ano: R\$
4.800.000,00

Segurança da Informação

A segurança da informação transcende a informática

Não existe sistema 100% seguro

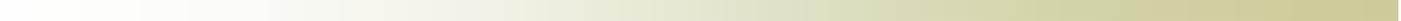
O elo mais fraco da corrente sempre será o ser humano

Os riscos e as vulnerabilidades transcendem o mundo tecnológico

Vulnerabilidades físicas, tecnológicas e humanas estarão sempre presentes

Questões

- Por que sistemas de informação são tão vulneráveis a destruição, erro, uso indevido e problemas de qualidade de sistemas?
- Que tipos de controles estão disponíveis para os sistemas de informação?
- Que medidas especiais devem ser tomadas para assegurar a confiabilidade, a disponibilidade e a segurança em processos de comércio eletrônico e negócios digitais?
- Quais são as técnicas mais importantes para garantir a qualidade de um software?
- Por que a auditoria dos sistemas de informação e a salvaguarda da qualidade dos dados são tão importantes?



SEGURANÇA EM TI

Tiago Alves de Oliveira

toliveira@divinopolisuemg.com.br