BOAS PRÁTICAS DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO (TI)

André Gustavo

Assessor Técnico de Informática

MARÇO/2012

Sumário

- Contextualização
- Definições
- Princípios Básicos de Segurança da Informação
- Ameaças (vulnerabilidades) à Segurança
- Principais Programas Maliciosos;
- Principais Golpes
- Mecanismos de Segurança
- Prevenções e Agentes de Segurança
- Boas práticas na utilização dos recursos de TI

Contextualização

- **Antigamente,** as informações eram armazenadas apenas em papel e a segurança era relativamente simples
- **Hoje**, com o constante avanço tecnológico, o uso cada vez maior de computadores e das redes, sobretudo a Internet e aplicações (***Processo Eletrônico, BL, Comunicação Eletrônica***), aspectos relacionados a segurança das informações estão mais complexos, exigindo equipes e métodos de segurança cada vez mais sofisticados
- 60% dos dados vazados de uma empresa é de responsabilidade do usuário da própria empresa. (*Fonte: CGI*)

Definições

- Informação
  - Conjunto de dados que possuem valor para um indivíduo ou organização
  - É o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe
- Segurança da Informação
  - Proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização

Princípios Básicos de Segurança da Informação

- Confidencialiade ou Privacidade
  - Garantia de que os dados só serão acessados somente por pessoas autorizadas (**sigilo, confidencial**)
- Disponibilidade
  - Garante que um sistema estará funcionando sempre que for requisitado (**estar disponível, acessível**)

Princípios Básicos de Segurança da Informação

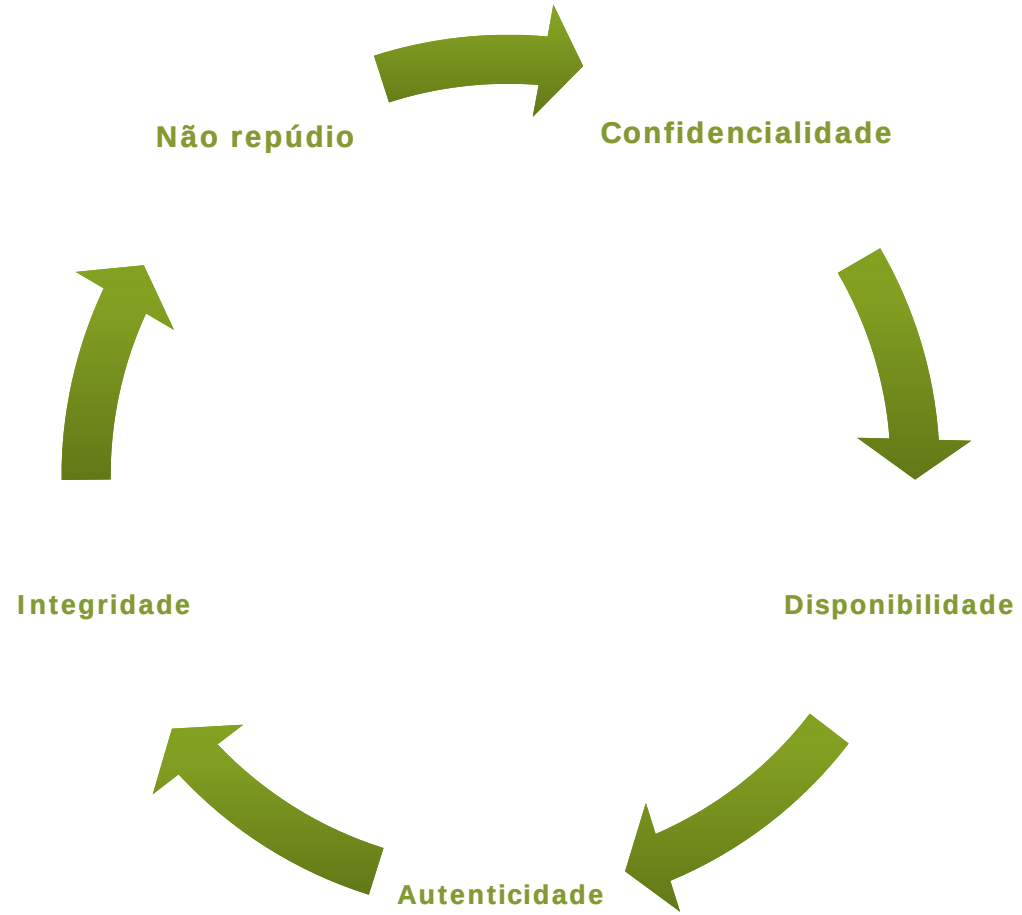
- Autenticidade
  - Garante a identidade de um usuário ou sistema com que se realiza uma comunicação (**ser autentico**, ou seja, ser ele mesmo)
- Integridade
  - Garante que uma mensagem (dado, e-mail, arquivo, etc) não foi alterado sem autorização (**ser íntegro**, manter-se o mesmo)
- Não Repúdio
  - Garante que um autor não consiga negar falsamente um ato ou documento de sua autoria. Isto é condição necessária para a validade jurídica de documentos e transações

Princípios Básicos de Segurança da Informação

... Tudo isso para manter a ...

- Confiabilidade
  - Garante que um sistema funcionará de forma eficiente e eficaz, de acordo com suas atribuições e funcionalidades (o sistema vai “cumprir seu papel”, vai fazer o que tem que fazer, no mínimo)

Princípios Básicos de Segurança da Informação



Ameaças (vulnerabilidades) à Segurança

- Defeitos de Hardware (Computadores, Servidores, Discos, etc)
- Facilidades no Acesso Físico
- Hackers (Usuários que invadem sistemas)
- Ataques Deliberados
- Spams (Emails Não Solicitados)
- **Malwares (Programas Maliciosos)**
- **Scams (Golpes)**

Principais Programas Maliciosos

- **Vírus**
  - É um programa que **se anexa a um arquivo hospedeiro** (ou seja, o vírus aloca seu código dentro do corpo do arquivo hospedeiro) e de lá tenta se copiar para outros arquivos. Só entra em ação quando seu arquivo hospedeiro é executado

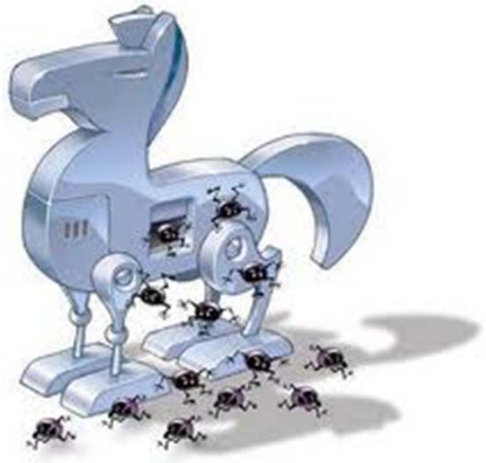
Computer	Name	Status	Date ...	Virus name	Size	Restoration folder	User
[redacted]	Flagratraicao.avi__www.msn-videos[1].com	Possibly infec...	28/1...	HEUR:Trojan.Win32.Generic	0	C:\Documents and Settings\machado\Configur...	TCE\[redacted]
[redacted]	rg9g9bgq.exe	Infected	24/2/...	Trojan-GameThief.Win32....	0	J:\rg9g9bgq.exe	TCE\[redacted]
[redacted]	janed.scr	Infected	11/1/...	Worm.Win32.VBNA.iwz	0	J:\janed.scr	
[redacted]	skata.class	Infected	19/1...	Trojan.Java.Payphish.a	0	C:\Documents and Settings\[redacted]\Con...	
[redacted]	UPX	Infected	13/1...	Trojan-Banker.Win32.BH...	0	C:\Documents and Settings\[redacted]\Con...	
[redacted]	UPX	Infected	13/1...	Trojan-Banker.Win32.BH...	0	C:\Documents and Settings\[redacted]\Con...	
[redacted]	os-cinco-sentidos-do-corpo-humano[1].htm	Infected	5/3/2...	Trojan.JS.Iframe.zw	0	C:\Documents and Settings\[redacted]\Con...	
[redacted]	i~139459.dl_	Infected	28/9/...	Trojan.Win32.KillAV.nh	0	C:\WINDOWS\system32\j~139459.dl_//i~139...	
[redacted]	JIM	Possibly infec...	19/1/...	HEUR:Trojan.Script.Iframer	0	C:\Documents and Settings\07822150413\Con...	
[redacted]	UPX	Infected	12/1/...	Trojan-Downloader.Win32...	0	E:\8585485\fernandaSilva.exe//UPX	TCE\[redacted]
[redacted]	video_Flag.wmv de www.maillive[1]...	Infected	5/3/2...	Trojan-Downloader.Win32...	0	C:\Documents and Settings\[redacted]\Con...	TCE\[redacted]
[redacted]	JIM	Possibly infec...	14/3/...	HEUR:Trojan.Script.Generic	0	C:\Documents and Settings\[redacted]\Con...	
SERVNT8	Th8tls4LvMyKttnln(trdçã).sCR	Infected	1/3/2...	Packed.Win32.Black.a	0	I:\[redacted]	
CLUSTER01-01	PMW-MT-CPRT-PDF-DEF.exe	Infected	29/9/...	Virus.Win32.Sality.aa	0	E:\BKP_Diario_INCREM\142-BKP_Cluster_Infor...	
CLUSTER01-01	PMW-MT-CPRT-PDF-DEF.exe	Infected	20/1...	Virus.Win32.Sality.aa	0	E:\$RECYCLE.BIN\S-1-5-21-2002014024-7114...	
[redacted]	A0004983.exe	Infected	11/1...	Packed.Win32.Klone.bq	180224	C:\System Volume Information_restore{A0EA...	

Principais Programas Maliciosos

- **Worm (Verme)**
  - É um programa é um **programa auto-replicante**. É projetado para tomar ações maliciosas após infestar um sistema, além de se auto-replicar, pode deletar arquivos em um sistema ou enviar documentos por email.

Principais Programas Maliciosos

- **Trojan (Cavalo de Tróia)**
  - É um **programa disfarçado** de um programa legítimo, que **esconde objetivos maliciosos**, como apagar dados, roubar informações e abrir portas de comunicação para que se possa invadir o computador.



Principais Programas Maliciosos

- **Spyware**
  - Programa que monitora as atividades de um sistema e envia as informações para terceiros.
  - **Keylogger**: Registra tudo o que é digitado pelo usuário e as envia para o invasor
  - **Screenlogger**: Registra em forma de imagem as teclas digitadas pelo usuário e as envia para o invasor.

Principais Golpes

- **Engenharia Social (HOAX)**
  - Tipo de golpe, pelo qual **alguém faz uso da persuasão**, muitas vezes abusando da ingenuidade ou confiança do usuário, **para obter informações** que podem ser utilizadas para ter acesso não autorizado a computadores ou informações

Principais Golpes

- **Phishing SCAM**
  - Tipo de g… **ou fazê-** para obte… etc
  - Normalm… através d… pertence…

Mecanismos de Segurança

- Controle Físico
  - São **barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura** (que garante a existência da informação) que a suporta. Ex: *Portas, salas, câmeras, guardas, prédios, muros, etc;*

- Controle Lógico
  - São **barreiras que impedem ou limitam acesso a informação, que está em ambiente controlado, geralmente eletrônico**, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado. Ex: *firewall, senha/pin, biometria, smartcards*

Prevenções para Segurança

- Realizar **Backup** em disco externo ou na nuvem (**cloud**), ou seja, em servidores remotos
- Possui **Antivirus** e **Anti-spyware** instalado e configurado para atualização automática e frequente
- Utilizar softwares (programas) originais
- Manter o sistema operacional (windows) sempre atualizado para corrigir eventuais falhas (**ativar atualizações automáticas no painel de controle**)

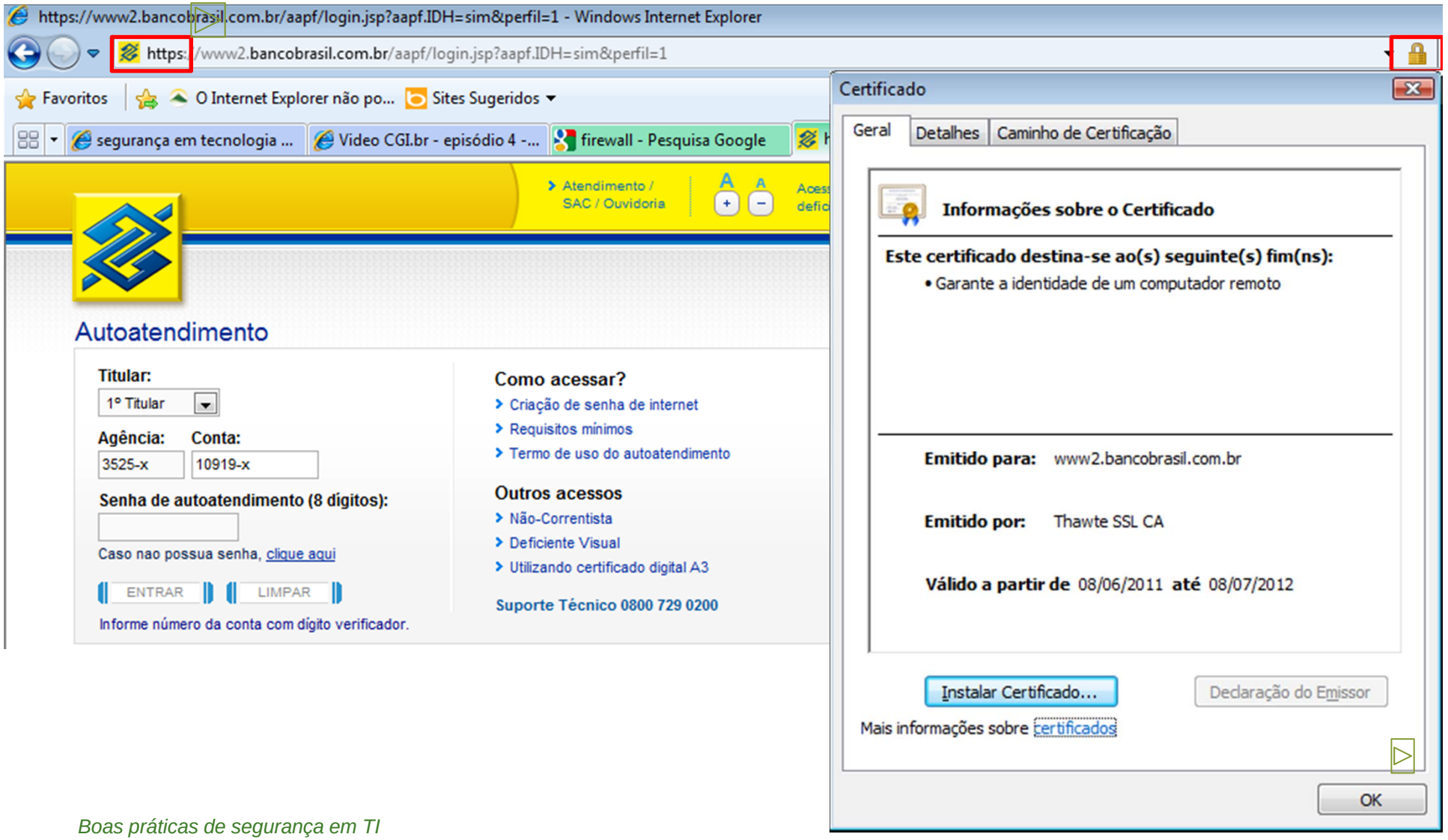
Anti-Spyware

- São programas cujo objetivo é tentar eliminar do sistema, através de uma varredura, spywares, keyloggers, trojans e outros malwares

Prevenções para Segurança

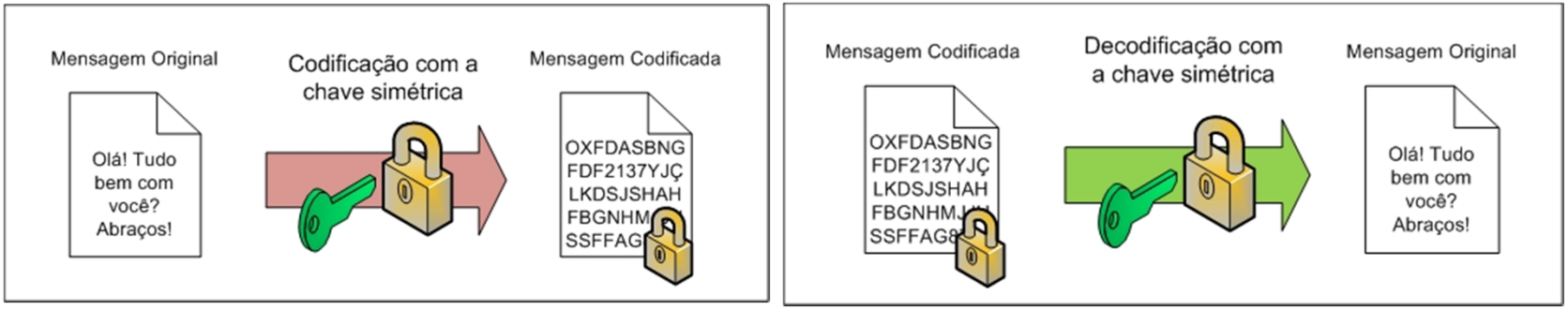
- Navegar conscientemente na Web
  - *Não clicar em links recebidos por e-mail*
  - Não executar arquivos anexados a e-mails, sem antes examiná-los
  - Evitar sites que pareçam suspeitos e não clicar em links de janelas Pop-ups
  - Utilizar **sites seguros** ao enviar dados confidenciais
- Utilizar **senhas** fortes em qualquer tipo de cadastro
- Utilizar **certificados digitais**
- Possuir **firewall** instalado e ativo (computador ou de rede)

Site Seguro

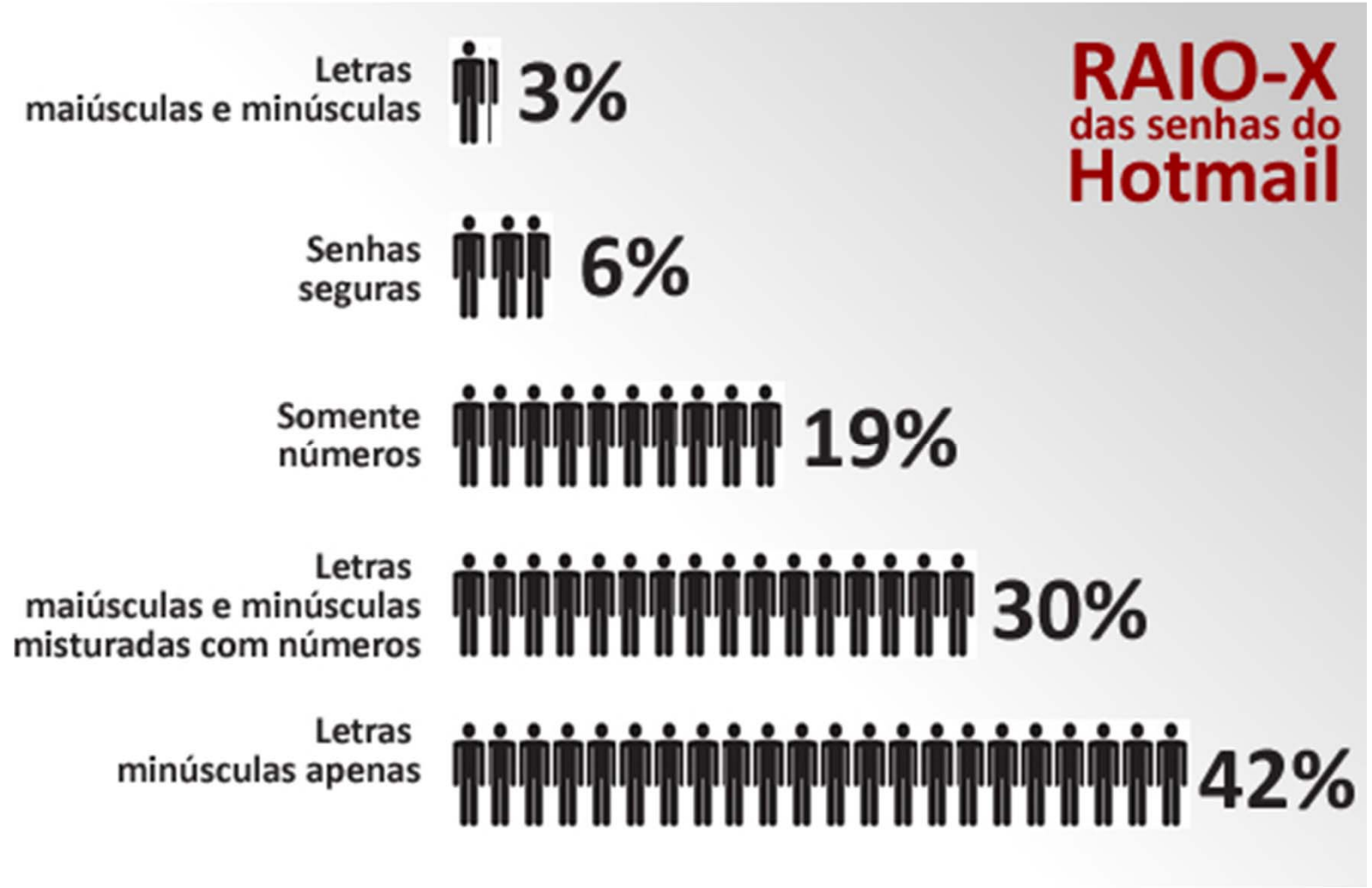

https://www2.bancobrasil.com.br/aapf/login.jsp?aapf.IDH=sim&perfil=1 - Windows Internet Explorer
https://www2.bancobrasil.com.br/aapf/login.jsp?aapf.IDH=sim&perfil=1
Favoritos
O Internet Explorer não po...
Sites Sugeridos
segurança em tecnologia ...
Video CGI.br - episódio 4 -...
firewall - Pesquisa Google
Atendimento / SAC / Ouvidoria
Autoatendimento
Titular:
1° Titular
Agência:
Conta:
3525-x
10919-x
Senha de autoatendimento (8 dígitos):
Caso nao possua senha, clique aqui
ENTRAR
LIMPAR
Informe número da conta com dígito verificador.
Como acessar?
Criação de senha de internet
Requisitos mínimos
Termo de uso do autoatendimento
Outros acessos
Não-Correntista
Deficiente Visual
Utilizando certificado digital A3
Suporte Técnico 0800 729 0200
Certificado
Geral
Detalhes
Caminho de Certificação
Informações sobre o Certificado
Este certificado destina-se ao(s) seguinte(s) fim(ns):
• Garante a identidade de um computador remoto
Emitido para: www2.bancobrasil.com.br
Emitido por: Thawte SSL CA
Válido a partir de 08/06/2011 até 08/07/2012
Instalar Certificado...
Declaração do Emissor
Mais informações sobre certificados
OK

Criptografia

- É uma técnica para tornar a informação ilegível, conhecida apenas pelo remetente e seu destinatário (detentores da "**chave secreta**"), o que a torna muito difícil de ser lida por alguém não autorizado.



Senhas


RAIO-X
das senhas do
Hotmail
Letras maiúsculas e minúsculas
3%
Senhas seguras
6%
Somente números
19%
Letras maiúsculas e minúsculas misturadas com números
30%
Letras minúsculas apenas
42%

Senhas

- Senhas longas e complexas. Ex: mínimo de 07 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais (ex: @ # $ % & *);
- Não utilizar nomes próprios, sobrenomes, datas de nascimento, parte do CPF, etc;
- Alterar regularmente por sua iniciativa própria ou de acordo com a política da instituição (Ex: a cada 30 dias);
- Política de senha do site ou organização
- Evitar salvar senhas em *cybercafé*, *Lan houses*, *redes sem fio* públicas;

Certificados Digitais

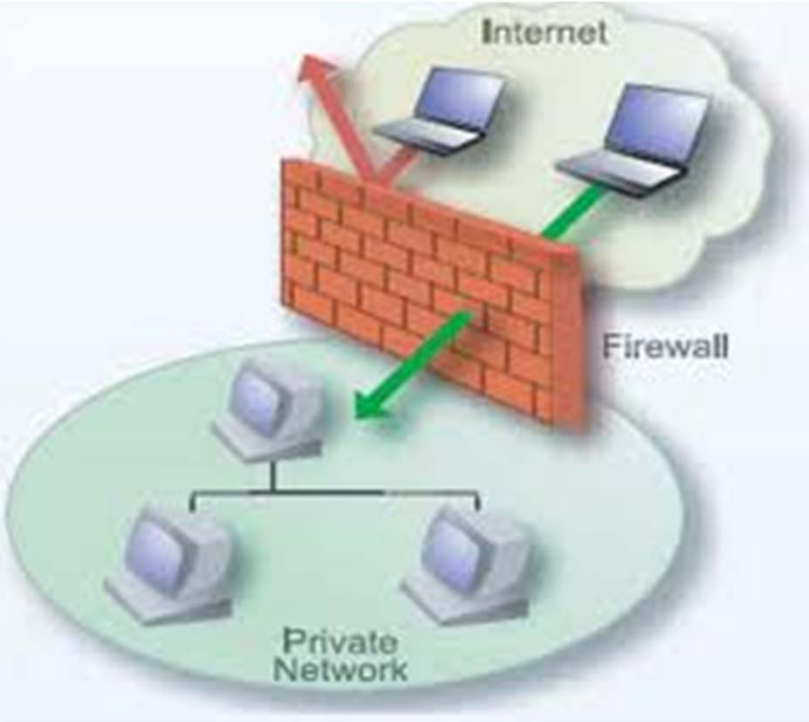
- É um documento eletrônico que contém informações que identificam uma pessoa, uma máquina ou uma organização na Internet. Este documento **garante a nossa identidade de forma incontestável**, porque está assinado digitalmente por uma a **Autoridade Certificadora** - AC, uma espécie de “Cartório Digital”).

Assinatura Digital

- É o recurso que permite associar uma mensagem a um autor, **garantindo a autoria e a integridade** da mensagem;
- É o equivalente a nossa assinatura real e autenticada, sendo que no mundo digital.
- Necessidade de utilização do **PIN** (Personal Identification Number)

Firewall

- Programa utilizado para **controlar/filtrar** o tráfego de entrada e saída de dados em uma rede.



Boas práticas na utilização de recursos de TI

- Desligue os computadores, monitores e impressoras ao final do expediente, depois os no-breaks e estabilizadores
- Encerre a sessão ou efetue o bloqueio da estação
- Evite o desligamento forçado
- Evite impressão desnecessária. Use arquivos **pdf**

Obrigado

André Gustavo
Assessor Técnico de Informática
andregustavo.rn@gmail.coam