

Gerenciamento de Segurança da Informação

Prof. Marcos Monteiro

<http://www.marcosmonteiro.com.br>

Agora!

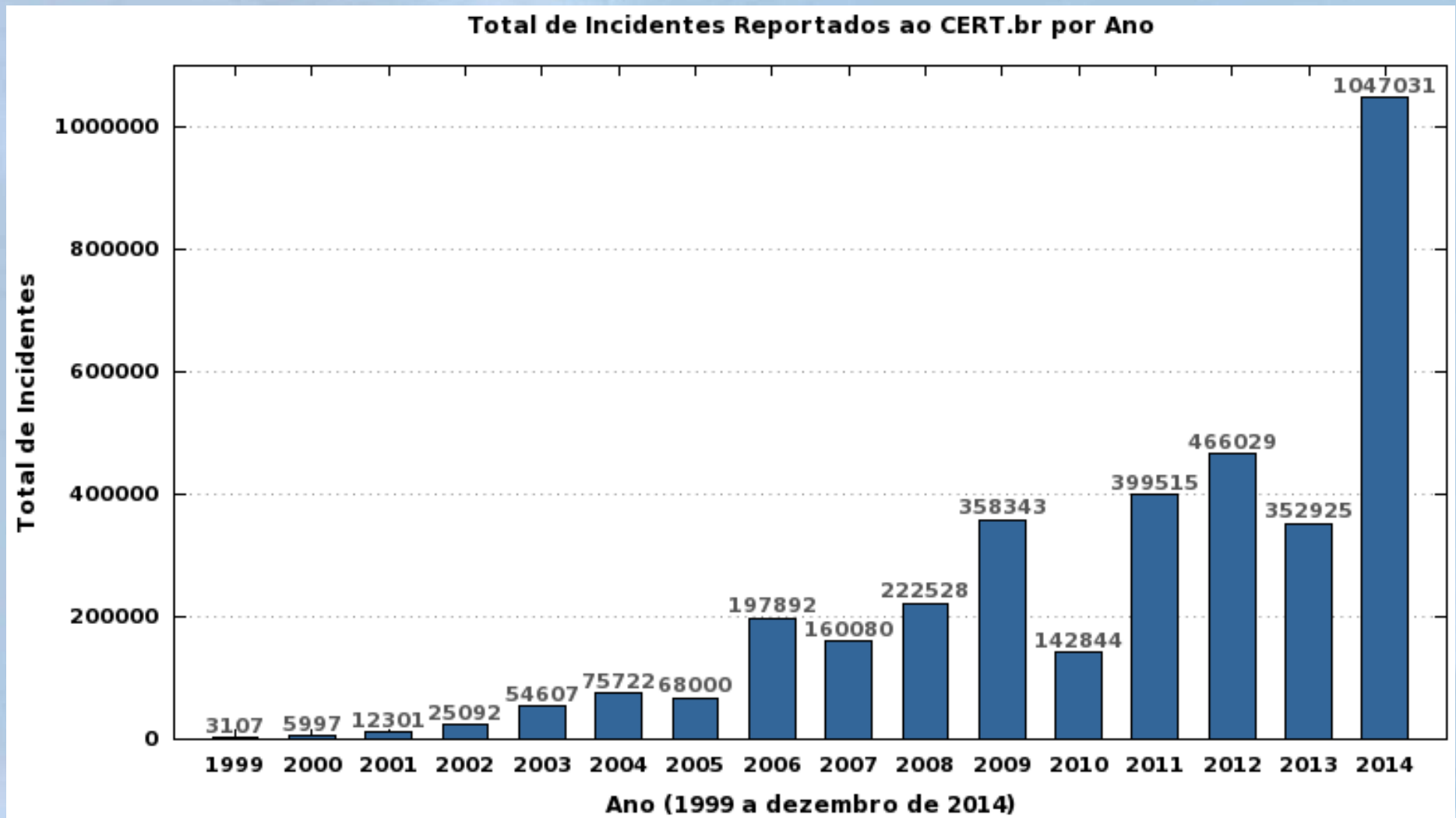


<http://map.ipviking.com>

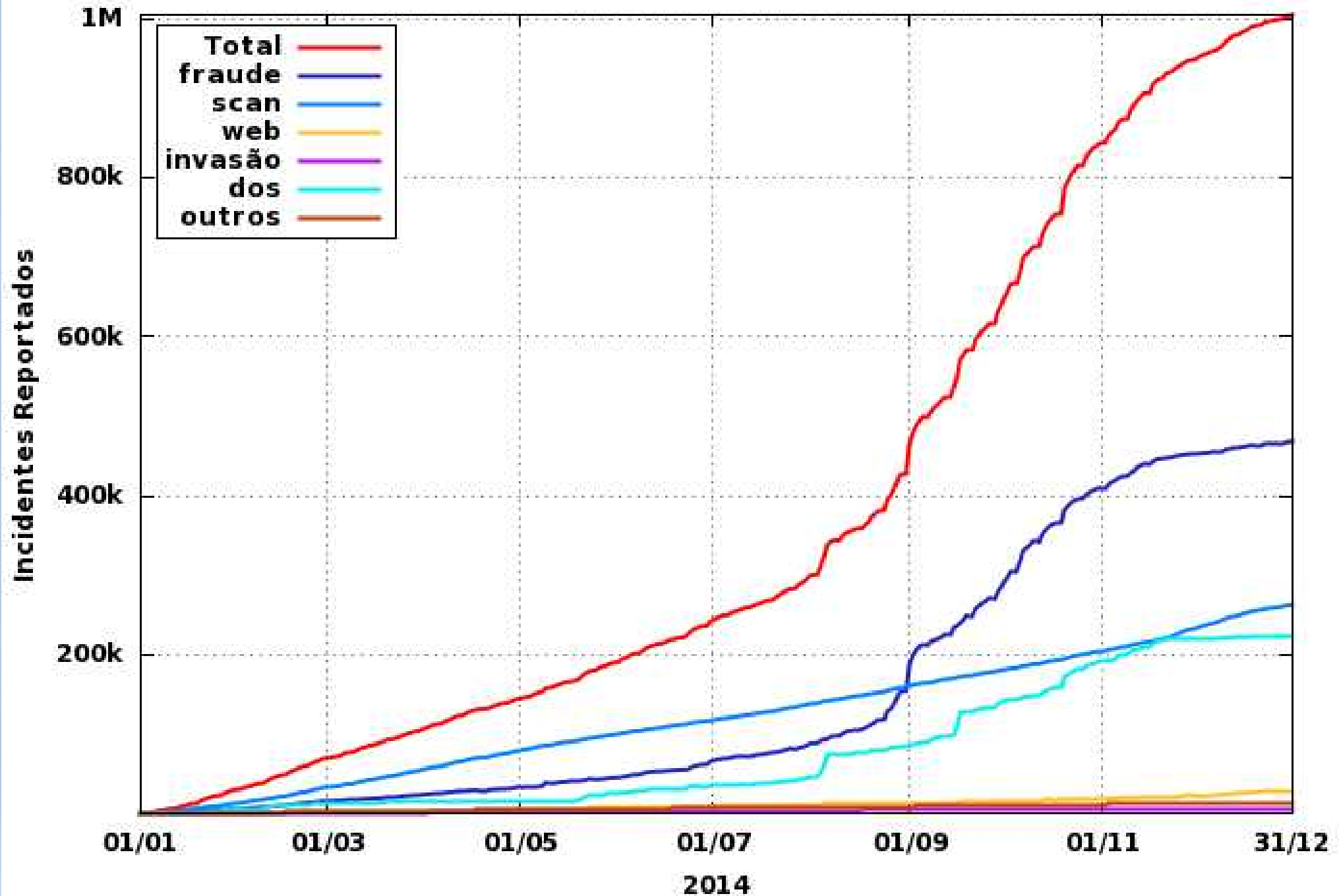
<http://cybermap.kaspersky.com/>



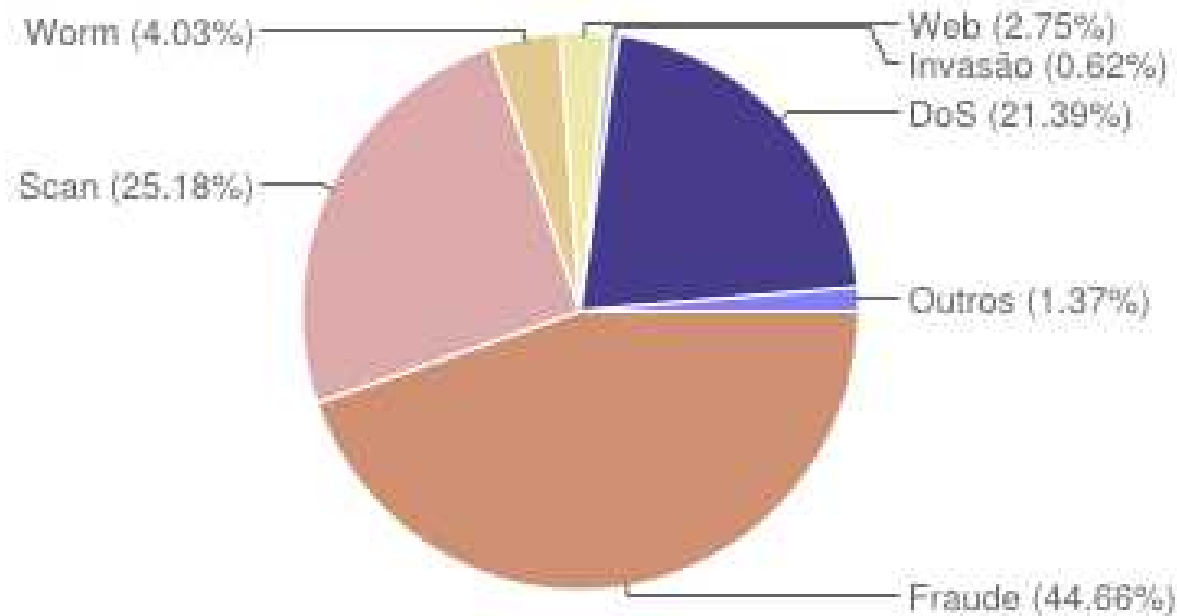
Centro de Estudos, Respostas e Tratamento de incidentes de Segurança do Brasil.



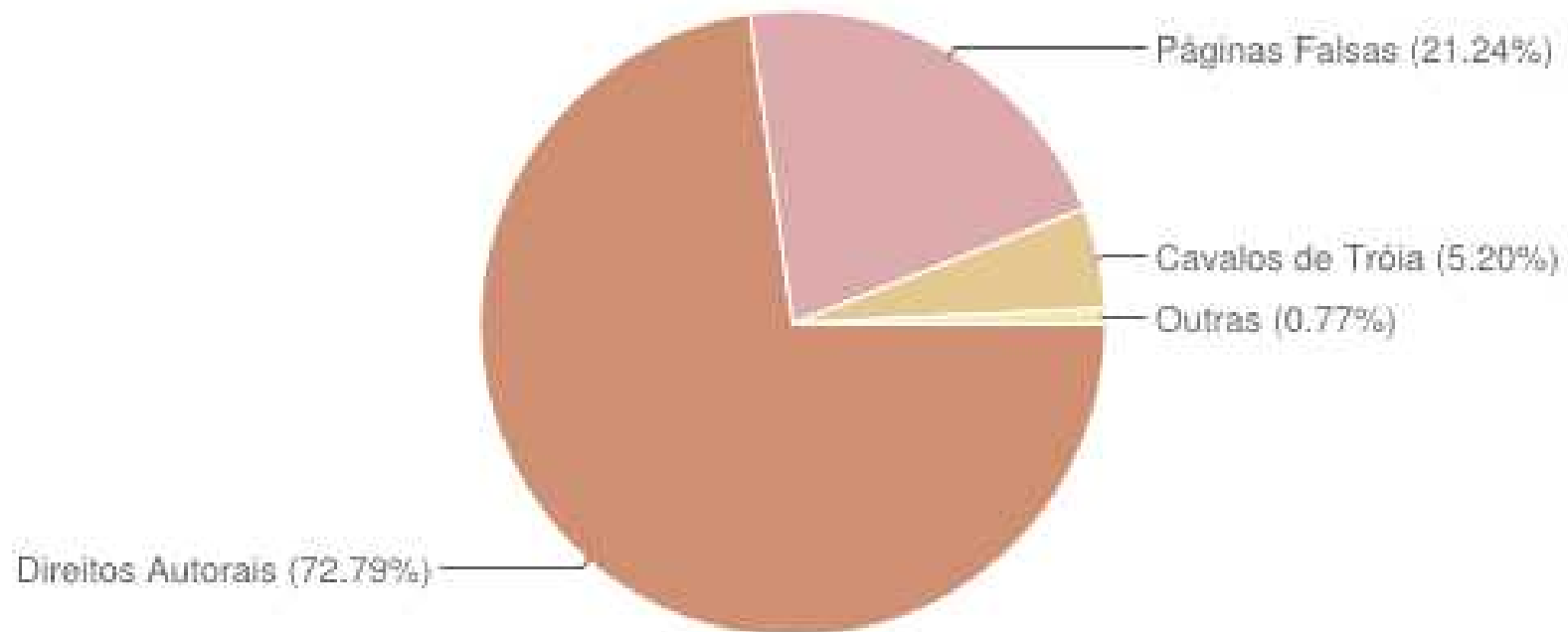
CERT.br: Incidentes Reportados (Tipos de Ataque Acumulado)



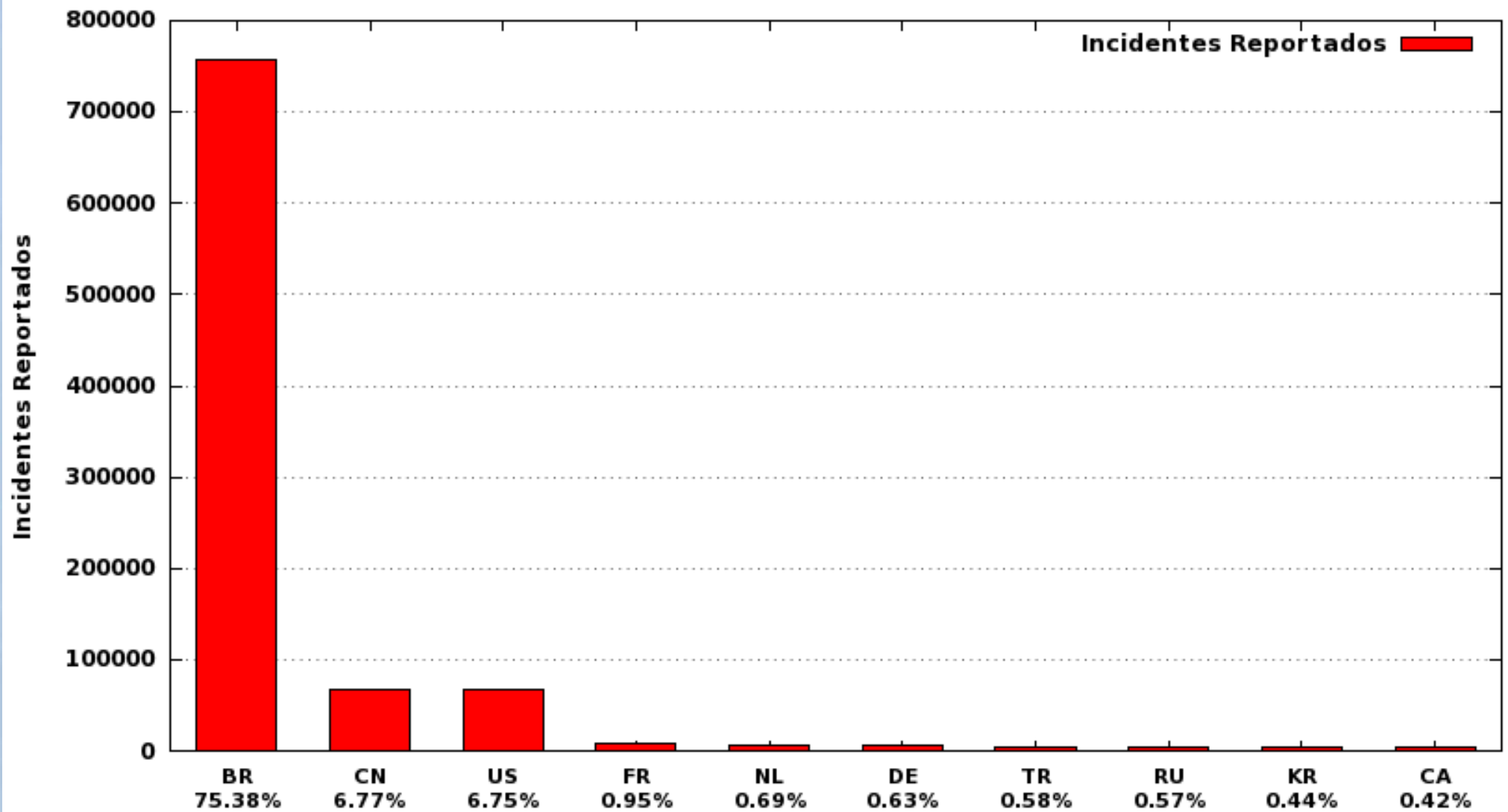
Incidentes reportados (Tipos de ataque)



Tentativas de fraudes reportadas



CERT.br: Incidentes Reportados (Top 10 CCs origem de ataques)



Hacker, Cracker, Lammer ?



Motivações

Trecho manifesto hacker: “Mas você já olhou por trás dos olhos de um hacker? Você já imaginou o que faz pulsar, que forças o deram forma, o que pode tê-lo moldado?”

Espionagem Industrial

Proveito Próprio

Vingança

Status

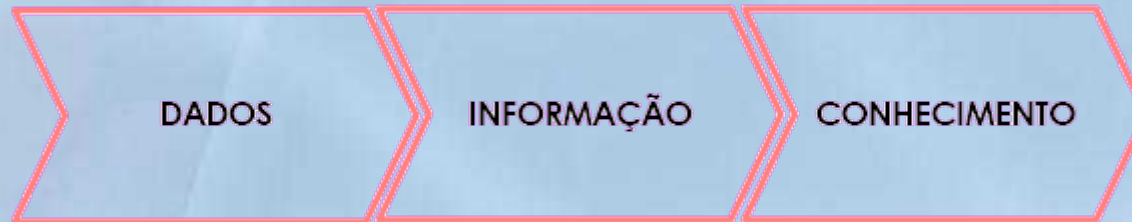
Aprendizado

Maldade

Desafios

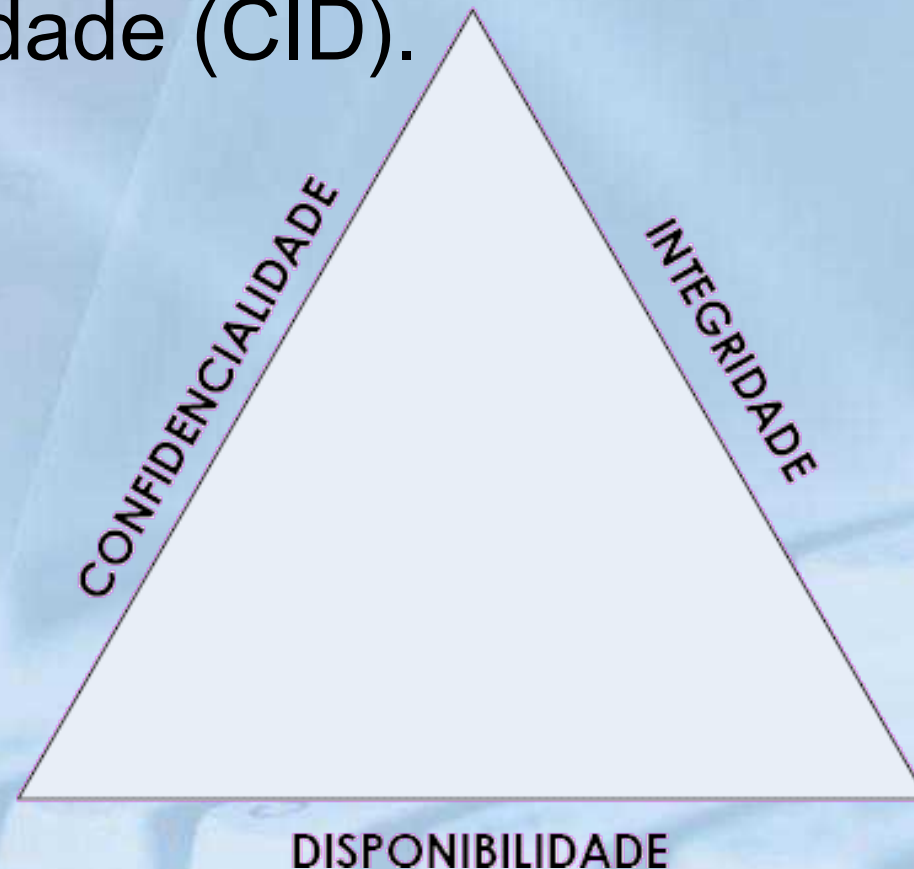
Ativo de informação

- A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor.



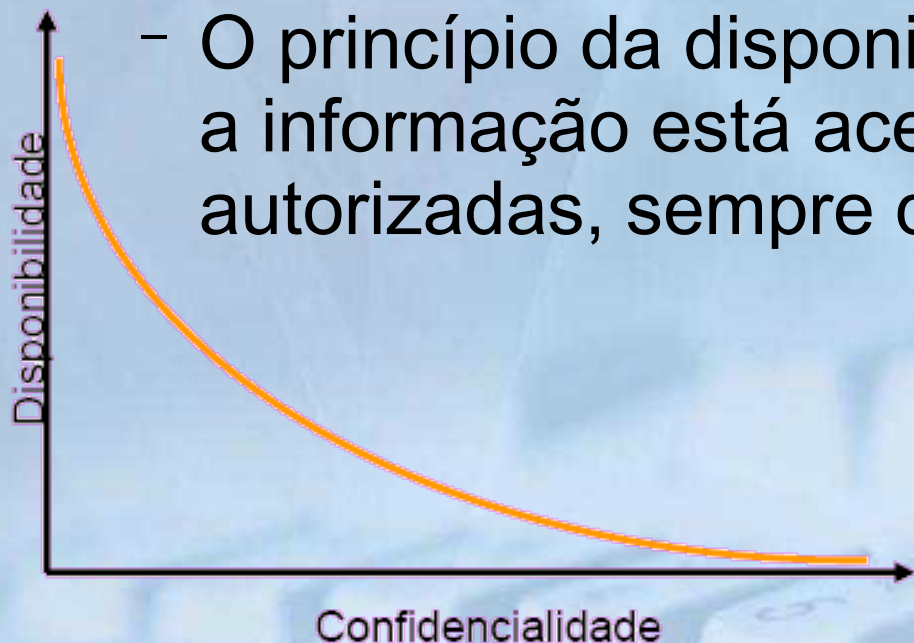
Propriedades de segurança da informação

- A segurança da informação é garantida pela preservação de três aspectos essenciais: confidencialidade, integridade, e disponibilidade (CID).



Disponibilidade X Confidencialidade

- Confidencialidade
 - O princípio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.
- Disponibilidade
 - O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.



- Integridade

- O princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável.

Disponibilidade

- Métricas

- Índice de disponibilidade do serviço =

- $\text{Tempo no ar} / \text{Tempo acordado} * 100$

- Analise de Impacto

- Utilidade para o negocio + No. Usuários Afetados + Disponibilidade Afetada

Vulnerabilidade

- São as fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade, e disponibilidade.

Vulnerabilidade

- “A Microsoft publicou 11 boletins de segurança em 13 de Abril que abordam ao todo 11 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código, escalação de privilégios de usuários locais conectados e negação de serviços.”
- Crítica
 - MS10-019: Vulnerabilidade no Windows Authenticode Verification
 - Vulnerabilidade que permite a execução remota de código

Ameaça

- A ameaça é um agente externo ao ativo de informação, que aproveitando-se das vulnerabilidades deste ativo, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação suportada ou utilizada por este ativo.

Ameaça

- Físicas e materiais
 - Incêndio, inundação, e outros desastres naturais;
 - Roubo de mercadorias/ produtos;
 - Falsificações.



Sala-cofre



A SALA-COFRE deve ser testada integralmente de acordo com normas específicas. O procedimento de certificação da ABNT/INMETRO PE047.01 regulamenta e exige a execução de diversos testes, segundo normas específicas que garantem o desempenho e conformidade da SALA-COFRE com as normas NBR 11515 e ISSO 27002. O Procedimento PE047.01 inclui também uma série de testes de fogo, calor e umidade para mitigar outros riscos existentes baseado na norma NBR 15427.

Ameaça

- Tecnológicas

- Uso indevido de recursos (rede, internet, telefone, etc);
- Malware: Vírus, Spyware, Worms.

- Intelectuais

- Engenharia Social
- Má conduta de funcionários
- Vazamento de informações e dados de clientes, fornecedores, funcionários e proprietários

Ameaça

Abrangência	Ameaça	Exemplo
Confidencialidade	<i>Browsing</i>	Procurar por informações sem necessariamente saber seu tipo
	<i>Shoulder surfing</i> ("papagaio de pirata")	Olhar sobre o ombro da pessoa o que é digitado.
	Engenharia Social	Fingir ser alguém com a intenção de ter acesso a informações.
Integridade	Modificar uma mensagem	Interceptar uma mensagem, alterá-la e enviá-la ao seu destino original
	Alteração de logs de auditoria	Modificar os logs de auditoria, normalmente com a intenção de ocultar fatos
	Modificação de arquivos de configuração	Alterar arquivos críticos em um sistema para modificar sua funcionalidade.
Disponibilidade	Desastres naturais ou provocados	Vandalismo, incêndios, terremotos, terrorismo, vulcanismo, ...
	Negação de serviço (DoS)	Comprometimento de serviços de importância fundamental para processos
	Comprometimento de informações	Modificar dados de forma a ficarem inúteis para outras pessoas

Ameaças de Antigamente



Chen-Ing Hau, 24
(Autor do vírus CIH)



Jeffrey Parson, 18
(autor do Blaster.B virus)



Joseph McElroy, 16
(Invadiu o laboratório de pesquisas nucleares dos EUA)



Kevin Mitnick

Cracker de 1970 a 1995
Consultor de Segurança hoje

Objetivos

- * Footprinting
 - intervalo de endereços do alvo
 - aquisição de espaço de nomes
 - obtenção de diversos detalhes do alvo
- * Varredura
 - avaliação em massa do alvo
 - serviços em escuta
- * Enumeração
 - contas válidas
 - recursos compartilhados
- * Ganho de acesso
 - coleta de informações mais particulares

Objetivos

- * Escalação de privilégios
obter controle total
- * Varreduras furtivas
novamente, processo de captura de informações
- * Encobrimento de rastros
ocultar fato dos administradores
- * Backdoors
garantir acesso futuro
- * Recusa de serviço
desabilitar o alvo

Técnicas

- * Footprinting
 - busca de código-fonte aberto
 - whois
 - interface web com o whois
 - transferência de zona DNS
- * Varredura
 - varredura ping
 - varredura portas tcp/udp
 - detecção de SO
- * enumeração
 - listagem de contas de usuários
 - listagem de compartilhamento de arquivos
 - identificação de aplicativos

Técnicas

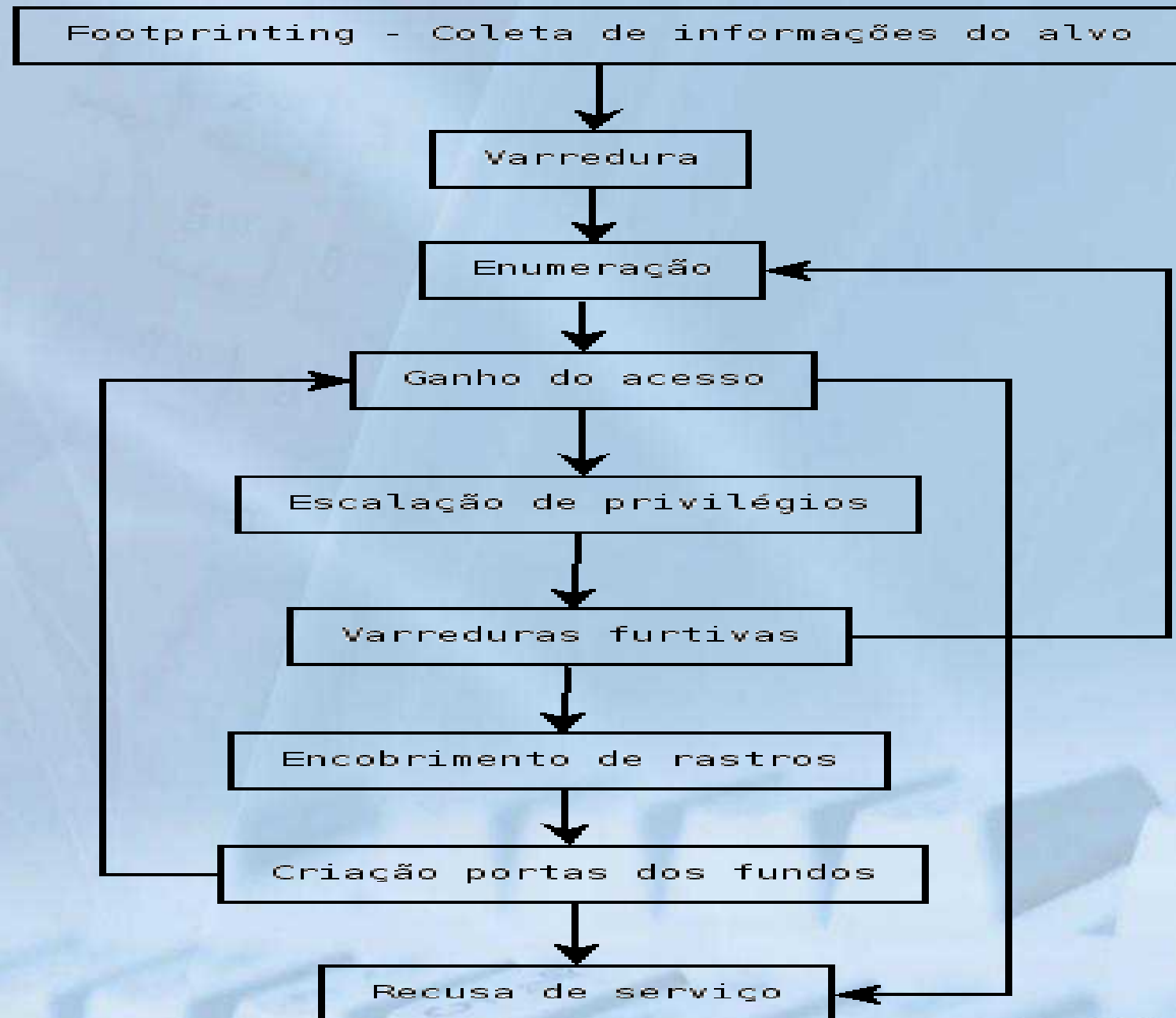
- * Ganho de acesso
 - escuta de senha
 - captura de arquivos de senha
 - estouros de buffer
- * Escalação de privilégios
 - decifração de senhas
 - explorações conhecidas
- * Varreduras furtivas
 - procura de senhas em texto puro
 - avaliação de relações de confiança
- * Encobrimento de rastros
 - limpeza dos logs
 - ocultar ferramentas

Técnicas

- * Criação de backdoors
criação de contas falsas
infecção de arquivos de inicialização
serviços de controle remoto
- * Recusa de serviço
inundação de SYN
técnicas ICMP
DDOS

Anatomia de um Ataque

A METODOLOGIA



Antes de conseguir ele deve ter tentado...

```
root@MM:~# tail /var/log/auth.log
Sep  3 00:48:47 MM sshd[12002]: pam_winbind(sshd:auth): request wbcLogonUser failed: WB
C_ERR_AUTH_ERROR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, E
rror message was: No such user
Sep  3 00:48:49 MM sshd[12002]: Failed password for root from 192.168.222.1 port 50126
ssh2
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): getting password (0x00000388)
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): pam_get_item returned a passwor
d
Sep  3 00:48:50 MM sshd[12002]: pam_winbind(sshd:auth): request wbcLogonUser failed: WB
C_ERR_AUTH_ERROR, PAM error: PAM_USER_UNKNOWN (10), NTSTATUS: NT_STATUS_NO_SUCH_USER, E
rror message was: No such user
Sep  3 00:48:53 MM sshd[12002]: Failed password for root from 192.168.222.1 port 50126
ssh2
Sep  3 00:48:53 MM sshd[12002]: Connection closed by 192.168.222.1 [preauth]
Sep  3 00:48:53 MM sshd[12002]: PAM 2 more authentication failures; logname= uid=0 euid
=0 tty=ssh ruser= rhost=macbook-air-de-marcos-local user=root
Sep  3 00:48:56 MM sshd[12005]: Accepted password for root from 192.168.222.1 port 5012
7 ssh2
Sep  3 00:48:56 MM sshd[12005]: pam_unix(sshd:session) session opened for user root by
(uid=0)
```

O novo atacante

- Silenciosos
 - Sem alarmes, sem vestígios
- Precisos
 - Personalização, códigos específicos
 - Tomam vantagem sobre fraquezas tecnológicas e humanas...

O que movimenta esse mercado?



Phishing

Pop ups
& BOs

Espionagem
Industrial

Sequestro de
browser

Roubo de
identidades

SPAM

Roubo de
dados
corporativos

Roubo de
Dados
pessoais

Problemas

- Segurança da Informação
 - Roubo/ furto de informações
 - Roubo/ furto de identidades
- Produtividade
 - Navegação improdutiva
 - SPAM
 - Sistemas desligados
 - Muitos chamados de Help desk
- Compliance
 - Falha no atendimento de leis e normas
- Imagem e consumidor
 - Referência da Marca
 - Reputação

Elo mais fraco!



Usuário “Clicador Feliz”



Acho que tenho que clicar em “sim”!

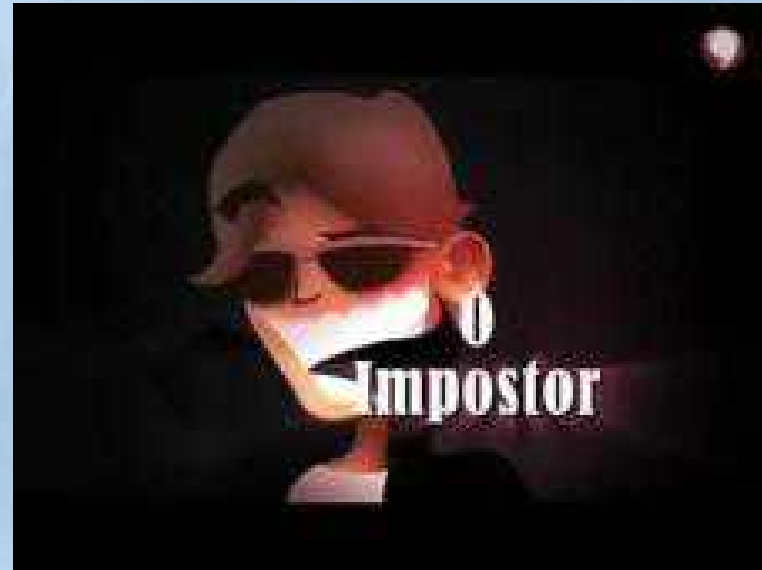


63% clicam em "Ok" sem pensar

- Psicólogos da Universidade do Estado da Carolina do Norte descobriram que usuários de computadores têm dificuldades para distinguir entre mensagens de alarmes falsos do Windows e as reais.
- Em uma experiência que testou a reação de 42 estudantes universitários usuários de internet, revelou-se que quase dois terços deles (63%) clicariam em "Ok" sempre que vissem uma pop-up de alerta, fossem falsas ou não.
- "Muitas pessoas caem nesse tipo de ataque por não reconhecer os elementos visuais que diferenciam as janelas de alertas falsos das reais", concluíram os pesquisadores.

- IDG Now, 25 de setembro de 2008

ENGENHARIA SOCIAL



Kevin Mitnick

Cracker de 1970 a 1995
Consultor de Segurança hoje

Na Internet

Gmail - CAIXA - Segurança. - microservice@gmail.com - Mozilla Firefox

Segurança. - ... X [https://mail.g...isp=inline&zw](https://mail.google.com/mail/?shva=1#inbox/132381af56bab2c7) X Correio :: Bem-vindo ao Horde X +

Google.com <https://mail.google.com/mail/?shva=1#inbox/132381af56bab2c7> Google

Google Docs Fotos Reader Web mais - microservice@gmail.com

Procurar e-mail Pesquisar na web [Mostrar opções de pesquisa](#)
[Criar filtro](#)

Novo Optimus 3D ds LG - www.lge.com/br - Primeira experiência em 3D no mundo Tri-Dual, NOVO LG Optimus 3D [Sobre estes anúncios](#)

Arquivar Spam Excluir + - Mover para ▼ Marcadores ▼ Mais ▼ 1 de 315

CAIXA - Segurança. Entrada | X

Internetbanking@caixa.gov.br para mim [mostrar detalhes](#) 02:41 (4 horas atrás) [Responder](#)

Cliente: CAIXA
E-mail: microservice@gmail.com.

 **Mensagem.html**
4K [Visualizar](#) [Baixar](#)

[Responder](#) [Encaminhar](#)

[internetbanking](#)
internetbanking@caixa.gov.br
[Mostrar detalhes](#)

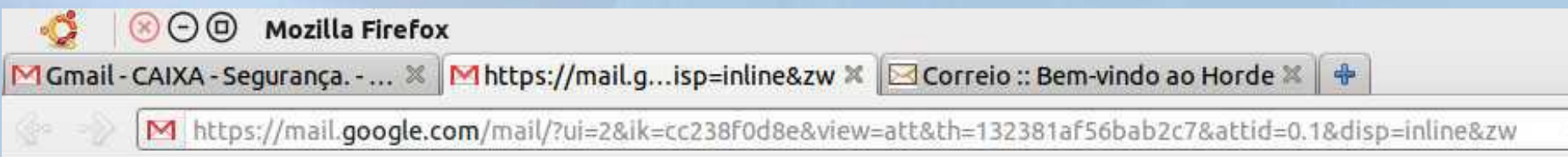
Anúncios

[Go for GMAT TOEFL MBA](#)
Complete prep, high level results
The Point for Success
www.thepointacademic.com.br/

[INSEAD's Top Ranked MBA](#)
Make One of your MOST important
Business Decisions. Your Career
www.insead.edu/Official

[MBA a distância Uninter](#)
MBA com professores especialmente
renomados. Inscrições Abertas!
www.PosEadUninter.com.br

[Online MBA Education](#)
British MBA Online Degree, 100%
Online in Just 12 Months, Apply
www.StudyInterActive.org



Prezado Cliente, microservice@gmail.com

Foi lançada uma nova correção para o Cadastramento de computadores, esta corrige uma falha em nível crítico do sistema de identificação do cliente, que pode ocasionar perdas de dados e problemas de acesso. A atualização é simples e rápida, basta entrar no link abaixo e em seguida acessar sua conta, e após completar todos os dados que pedirão para efetuar uma atualização completa.

Para iniciar a atualização siga o caminho abaixo:

https://Internetbanking.caixa.com.br/k0vmog2/Index_processa

Atenção: Todos os usuários devem se cadastrar e atualizar o Cadastramento de Computadores. Caso a correção não seja realizada, seu computador será bloqueado e o desbloqueio só poderá ser realizado nas agências da CAIXA.



Já possuo usuário

Usuário:

Acessar como:

- ☐ Pessoa Física
☐ Pessoa Jurídica
☐ Governo

Ir para:

Página Inicial ▾

CONFIRMAR



VEM QUE
TÁ NA MÃO

Clique e saiba mais







Identificação do usuário

para acessar o Internet Banking CAIXA informe a Senha Internet.

Senha Internet:

[Esqueci minha senha](#)

LIMPAR SENHA

CONFIRMAR

Utilize o teclado virtual para inserir sua senha,
é segurança dobrada para seu relacionamento.

Marque seu teclado virtual

1	2	3	4	5	6	7	8	9	0
q	w	e	r	t	y	u	i	o	p
↑	a	s	d	f	g	h	j	k	l
CAPS	z	x	c	v	b	n	m	←	



Banco CAIXA - Recadastramento - Mozilla Firefox

Gmail - CAIXA - Segurança. - ... X https://mail.g...isp=inline&zw X Banco CAIXA - Recadastram... X Correio :: Bem-vindo ao Horde X

http://phudau.com/ /internetbanking.caixa.gov.br/Cad_Computer.php

Google



Atualização de dados Cadastrais

Informe os dados abaixo para realizar a atualização dos dados cadastrais de sua conta.

CPF: (somente números)

Agência/Operação/Conta: / /

Senha do Cartão: (Senha de 4 dígitos)

[RETORNAR](#) [CONTINUAR](#)

* Para contas de Pessoa Física ou Pessoa Jurídica devem ser informados os dados do titular/representante legal, conforme cadastro na Receita Federal..



<http://phudau.com/ /internetbanking.caixa.gov.br/img/btoRetornar.gif>

CAIXA - O banco que acredita nas pessoas - Mozilla Firefox

Gmail - CAIXA - Segurança. - ... x https://mail.g...isp=inline&zw x CAIXA - O banco que acredi... x Correio :: Bem-vindo ao Horde x

http://www.caixa.gov.br/ Google

CAIXA O banco que acredita nas pessoas

VOCÊ CLIENTE [ACESSE SUA CONTA](#)

▼ MENU REDE DE ATENDIMENTO SOBRE A CAIXA CAIXA CULTURAL DOWNLOADS OUVIDORIA FALE CONOSCO

VOCÊ EMPRESAS GOVERNO JUDICIÁRIO

Aplicações Financeiras
Bolsa Família
CAIXA Celular
Cartão de Débito
Cartões de Crédito
Certificação Digital
Consórcios CAIXA
Conta CAIXA Fácil
Conta Corrente Pessoa Física
Contribuição Sindical Urbana

Consignação CAIXA
Cheque Especial
Crédito
DDA CAIXA
Investimentos
PIS
Poupança
Previdência Privada
Seguros
Seguro Desemprego

ÁREAS ESPECIAIS

- CAIXA Internacional
- Feirão CAIXA
- Imóveis a Venda
- Imprensa
- Portal de Compras
- Turismo
- Universitário
- Vitrine de Joias CAIXA

► Veja todos os produtos e serviços para você

Habitação, Simulador, Documentação
FGTS, Extrato, CRF, FGTS no Celular

Buscar por: Digite um texto

FOLHA CAIXA WEB

FOLHA CAIXA WEB

O **SALÁRIO** DOS SEUS EMPREGADOS EM DIA, DE FORMA **FÁCIL E SEGURA**

- Gerenciamento Seguro
- Transações pelo IBC
- Facilidade na operação
- Tudo sobre Folha CAIXA Web

POUPANÇA

PLANEJE O SEU SONHO COM A POUPANÇA CAIXA.

- Poupança CAIXA
- Programe sua Poupança
- História da Poupança
- Poupança Empresa
- Tudo sobre Poupança

LOTÉRIAS

MEGA-SENA

Concurso 1316
3/9/2011

08 - 13 - 25 - 34 - 42 - 48

- Loterias pelo celular
- Confira os Últimos resultados
- Tudo sobre Loterias

Cotações em tempo real no seu celular ou iPad.

Conectado a www1.caixa.gov.br...

Welcome to Phũ Đầu - Mozilla Firefox

Gmail - CAIXA - Segurança. - ... x https://mail.g...isp=inline&zw x Welcome to Phũ Đầu x Correio :: Bem-vindo ao Horde x

http://phudau.com/ Google

Monday Sep 05th Text size + x -



TRANG CHỦ NGHỆ THUẬT SỐNG HỌ LÃ AI GIÁO DỤC CHUYỆN CƯỜI BLOG VIDEO CLIP XẾP GIẤY ẢNH VUI LIÊN HỆ

HEADLINE

When You Tell Me That You Love Me

I wanna call the stars
Down from the sky
I wanna live a day
That never dies
I wanna change the world
Only for you
All the impossible
I wanna do

NGHỆ THUẬT SỐNG

Chìa khóa dẫn đến thành công



(Dân trí) - Chuyên gia nghề nghiệp Caryl Chessman chia sẻ: "Nếu tôi phải chọn 3 tiêu chí quan trọng quyết định đến thành công của một người thì niềm tin, hành động và kỷ luật là sự lựa chọn của tôi..."

MORE:

- Cảm ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân

LỜI HAY Ý ĐẸP

Christopher Lehmann Haunt

Nghệ thuật sống

- Chìa khóa dẫn đến thành công
- Cảm ơn đời mỗi sớm mai thức dậy...
- 19 điều tự nói với bản thân
- Ngày của Mẹ (Mother's Day)
- Hạnh phúc và bất hạnh

Bài viết xem nhiều nhất

- Tôi yêu em đến nay chúng có thể
- 100 Điều Lãng Mạn Cho Người Ấy !!!!!!!
- Thế giới mèo yêu
- Những hình ảo giác
- Edison - "Thiên tài là một phần trăm cảm hứng và 99 phần trăm đổ mồ hôi"
- Beethoven - Thiên Tài Vượt Lên Trên Số Phận
- Những trận đấu võ đài

Giải trí

- Những luật lệ lạ đời nhất thế giới
- BIẾT TÔI LÀ AI KHÔNG
- PHIL COLLINS - TRUE COLORS
- Ranh ngôn công chức
- Khi "thằng nhỏ" đòi tăng lương

Clip vui

- That is love
- Another Day in Paradise
- Graduation (Friends Forever) - Vitamin C
- Jeff Dunham & Peanut
- heaven's lunch

Giáo dục

- Tam Giác Thông Minh
- Những câu hỏi buồn cười nhất trên Yahoo
- Khích lệ bài 5

Who's Online



Index of / - Mozilla Firefox



Gmail - CAIXA - Segurança. ...

https://mail....isp=inline&zw

Index of /

404 Not Found

Correi



http://phudau.com/ /



Google

Index of /

- [Parent Directory](#)
- [elite.php](#)
- [http-internetbanking.caixa.gov.br/](#)
- [https-internetbanking.caixa.gov.br/](#)
- [internetbanking.caixa.gov.br/](#)

Apache Server at phudau.com Port 80

phudau.com - phpshell - Mozilla Firefox

Gmail - CAIXA - Segurança. ... https://mail....isp=inline&zw phudau.com - phpshell 404 Not Found Correio :: Bem-vindo ao Ho...

http://phudau.com/ /elite.php

C99Shell v. 1.0 pre-release build #16

Software: Apache, PHP/5.2.17
 uname -a: Linux box304.bluehost.com 2.6.32-42.1.BHsmpp #1 SMP Tue Jun 28 17:06:41 MDT 2011 x86_64
 uid=1412(kinghelp) gid=1410(kinghelp) groups=1410(kinghelp)
 Safe-mode: OFF (not secure)
 /home2/kinghelp/public_html/phudau.com/ / drwxr-xr-x
 Free 1365.8 GB of 1833.41 GB (74.5%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Insideteam Corporation - 2010

Listing folder (1 files and 3 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	04.09.2011 20:48:39	kinghelp/kinghelp	drwxr-xr-x	 
..	LINK	04.09.2011 20:26:18	kinghelp/kinghelp	drwxr-xr-x	 
[http-internetbanking.caixa.gov.br]	DIR	04.09.2011 20:50:37	kinghelp/kinghelp	drwxr-xr-x	 
[https-internetbanking.caixa.gov.br]	DIR	04.09.2011 20:50:41	kinghelp/kinghelp	drwxr-xr-x	 
[internetbanking.caixa.gov.br]	DIR	04.09.2011 20:50:32	kinghelp/kinghelp	drwxr-xr-x	 
elite.php	161.71 KB	04.09.2011 20:46:51	kinghelp/kinghelp	-rwxr-xr-x	  

:: Command execute ::

Enter:

Select:

:: Shadow's tricks :D ::

Useful Commands

Kernel version

Warning, Kernel may be alerted using higher levels

Kernel Info:

Linux box304.bluehost.com 2

:: Preddy's tricks :D ::

E-mail: É de que??



Comunicamos que o Itau está realizando a atualização e correção da sua
for <microservice@gmail.com>
(version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Thu, 15 Jan 2015 15:00:50 -0800 (PST)
Received-SPF: fail (google.com: domain of internetbanking@itau.com.br does not designate 209.208.110.35 as permitted sender) client-ip=209.208.110.35;
Authentication-Results: mx.google.com;
spf=fail (google.com: domain of internetbanking@itau.com.br does not designate 209.208.110.35 as permitted sender) smtp.mail=internetbanking@itau.com.br;
dkim=temperor (no key for signature) header.i=0;
dmarc=fail (p=NONE dis=NONE) header.from=itau.com.br
Received: from [127.0.0.1] (port=59322 helo=bloc.digimnt.com.br)
by painel.cloudalive.com.br with esmtp (Exim 4.84)
(envelope-from <internetbanking@itau.com.br>)
id 1YBtPG-0007IO-HZ
for contato@marcosmonteiro.com.br; Thu, 15 Jan 2015 20:00:50 -0300
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=adkl; d=itau.com.br;
h=Date:From:To:Subject:Reply-To:Message-ID:Mime-Version:Content-Type; i=internetbanking@itau.com.br;
bh=t6y1EmmrVaQxy5xHPy3KSj3FOEw=;
b=YPOX3JCzUPo2C6XuyQ49kupczaS43n+7tIHtaKsYkncR6QGzQaYFEI2PESRQItpzSu0EJk3wz2xs
YRcWxaWkxLxDkQ9g50keXAJdDDfXUJSR7lyf0flbOegBRQn/eP0InbpDDrUPoVNpnqEJk93dzQcB
ldEtFaDLyq2Poa/zlLc=
DomainKey-Signature: a=rsa-sha1; c=noews; q=dns; s=adkl; d=itau.com.br;
b=NxBgc8jnQrR3RXLa12wygTouVYLRRGSTli0Loxaudh0ZOPf52http/IjVEpzG13o4nHSQKJAI+i4X
LPcFv1CZU46FleVsrVI48Vw3ZqPFZEE9N60zoz2jgbcAvwI0H9QevRSZTluXgS07VYVTBBI0SfY
xrQZGA+PAAKLIs7wkNc=;
User-Agent: CodeIgniter
Date: Thu, 15 Jan 2015 21:00:46 -0200
From: "Itau S/A" <internetbanking@itau.com.br>

E-mail 3 – Remetente fraudado

Delivered-To: microservice@gmail.com
Received: by 10.216.52.193 with SMTP id e43csp120080wec;
Thu, 4 Dec 2014 15:09:47 -0800 (PST)
X-Received: by 10.194.193.38 with SMTP id hl6mr19710174wjc.38.1417734587188;
Thu, 04 Dec 2014 15:09:47 -0800 (PST)
Authentication-Results: mx.google.com;
spf=softfail (google.com: best guess record for domain of transitioning
apache@access3.thairegister.com does not designate <unknown> as permitted sender)
smtp.mail=apache@access3.thairegister.com
Received-SPF: softfail (google.com: best guess record for domain of transitioning
apache@access3.thairegister.com does not designate <unknown> as permitted sender)
Message-ID: <5480e9bb.523b7c0a.1b54.ffffe56cMFETCHER_ADDED@google.com>
Received: by 10.124.59.82 with POP3 id l18mf10309243wgh.21;
Thu, 04 Dec 2014 15:09:47 -0800 (PST)
X-Gmail-Fetch-Info: contato@marcosmonteiro.com.br 5 mail.marcosmonteiro.com.br 110
contato@marcosmonteiro.com.br
Return-path: <apache@access3.thairegister.com>
Envelope-to: contato@marcosmonteiro.com.br
Delivery-date: Thu, 04 Dec 2014 19:56:22 -0300
Received: from [127.0.0.1] (port=42776 helo=access3.thairegister.com)
by painel.cloudalive.com.br with esmtp (Exim 4.84)
(envelope-from <apache@access3.thairegister.com>)
id 1XwfJt-0004mI-QC
for contato@marcosmonteiro.com.br; Thu, 04 Dec 2014 19:56:22 -0300
Received: by access3.thairegister.com (Postfix, from userid 48)
id BE01419B133E; Fri, 5 Dec 2014 05:31:06 +0700 (ICT)
To: contato@marcosmonteiro.com.br
Subject: contato@marcosmonteiro.com.br - Seus pontos vencem hoje. Realize agora o resgate
e a troca de seus pontos pelos melhores premios nas melhores lojas. PROMO201427541
MIME-Version: 1.0
Date: Thu, 04 Dec 2014 15:09:47 -0800 (PST)
From: contato@marcosmonteiro.com.br

Content-type: text/html; charset=iso-8859-1

From: Programa de Vantagens Cielo <fidelidade13947@programadepremiosdezembro.com.br>
Message-Id: <20141204223107.BE01419B133E@access3.thairegister.com>

O IP 10.216.52.193 enviou um e-mail utilizando o usuário "apache@access3.thairegister.com", com certeza invadiram ou estão utilizando uma vulnerabilidade do Plesk Panel do site <http://www.thairegister.com>. Como o usuário é chamado de apache, deve haver algum script em PHP enviando e-mails, com isso ele pode facilmente alterar o cabeçalho da mensagem que será entregue.

O possível invasor pode ter conseguido acessar o painel por este link: <http://access3.thairegister.com:8880/> e como vimos a página está padrão de instalação, é bem possível que o usuário e a senha esteja padrão também.

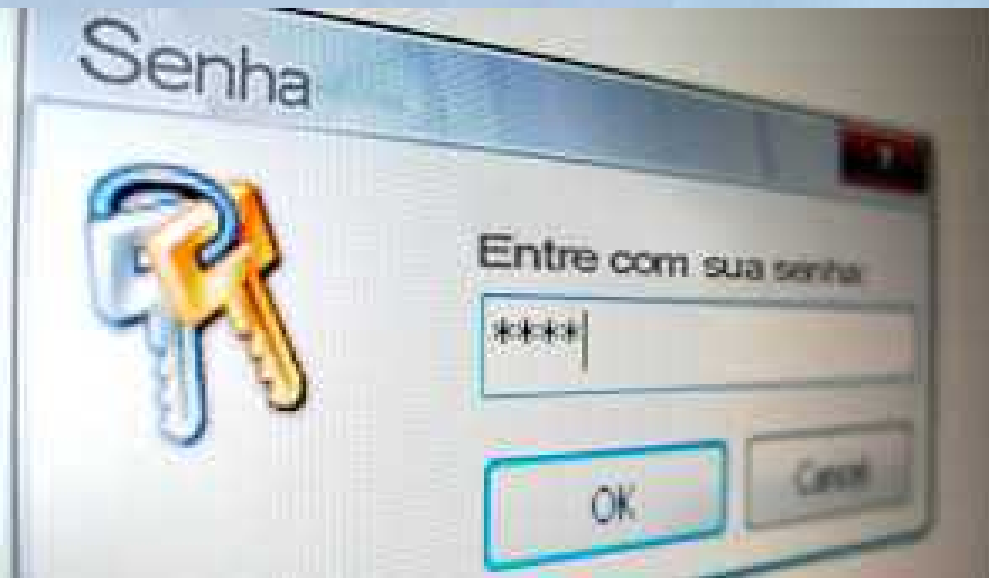
Crime

- Lei 3.914/1941

"Art 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa..."

É crime!

- ...usar a senha de outra pessoa também pode ser:
- Falsa Identidade (art.307 do Código Penal):
 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
 - Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.



**odeio a Joana silva**
(9 membros)

- [participar](#)
- [denunciar abuso](#)

- [fórum](#)
- [enquetes](#)
- [eventos](#)
- [membros](#)

odeio a Joana silva

[Início](#) > [Comunidades](#) > [Pessoas](#) > odeio a Joana silva

descrição: COMU FEITA PRA QUEM ODEIA A JOICE

idioma: **Português (Brasil)**

categoria: [Pessoas](#)

dono: joana silva

tipo: pública

privacidade do conteúdo: aberta para não-membros

local: rio de janeiro, rj, 222222, Brasil

criado em: 25 de junho de 2007

membros: 9

membros (9)**eu odeio a vaca da Lara Regina**
(23 membros)

- [participar](#)
- [denunciar abuso](#)

- [fórum](#)
- [enquetes](#)
- [eventos](#)
- [membros](#)

eu odeio a vaca da Lara Regina

[Início](#) > [Comunidades](#) > [Outros](#) > eu odeio a vaca da Lara Regina

descrição: dispeitada, invejosa, gorenta, avarenta, mau amada,gorda, asquerosa e ainda é feia, fejoada...feia e enjoada...ahahhahahahahah

idioma: **Português (Brasil)**

categoria: [Outros](#)

dono: vaca safada

tipo: pública

privacidade do conteúdo: aberta para não-membros

local: varjao, goias, 740000, Brasil

criado em: 6 de junho de 2006

membros: 23

- Ameaça (art. 147 do Código Penal):
 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa.
- Calúnia (art. 138 do Código Penal):
 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
 -
- Difamação (art. 139 do Código Penal):
 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.
 -
- Injúria (art. 140 do Código Penal):
 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.

- Quem aqui a mamãe disse:

***“Não pegue o que
não é seu !!!”***



... e “não dê CTRL+C e CTRL+V no conteúdo alheio” ?

Art. 184, Código Penal

Violar direitos de autor e os que lhe são conexos.

Pena:

detenção, de **3 (três) meses**
a **1 (um) ano**, ou multa
(SEM LUCRO)

reclusão, de **2 (dois) a 4**
(quatro) anos, e multa.
(COM LUCRO)

Art. 29, Lei 9610/98

Depende de autorização
prévia e expressa do autor
a **utilização da obra**, por
quaisquer modalidades, tais
como:

(...)

VI - a **distribuição**, quando
não intrínseca ao contrato
firmado pelo autor
com terceiros para uso ou
exploração da obra.

...até fofoca pode ser crime!

- Art. 154 do Código Penal - Decreto Lei 2848/40
 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
 - Pena - detenção, de três meses a um ano, ou multa.



Caso Carolina Dieckmann





“Lei Carolina Dieckmann” (PL 35/2012) Lei Nº 12.737, de 30 de Novembro de 2012

- Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
- Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:



“Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.



§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”



“Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”

Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.





Passa a vigorar a seguinte redação: Art. 266

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública





Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

Equipara-se a documento particular o cartão de crédito ou débito

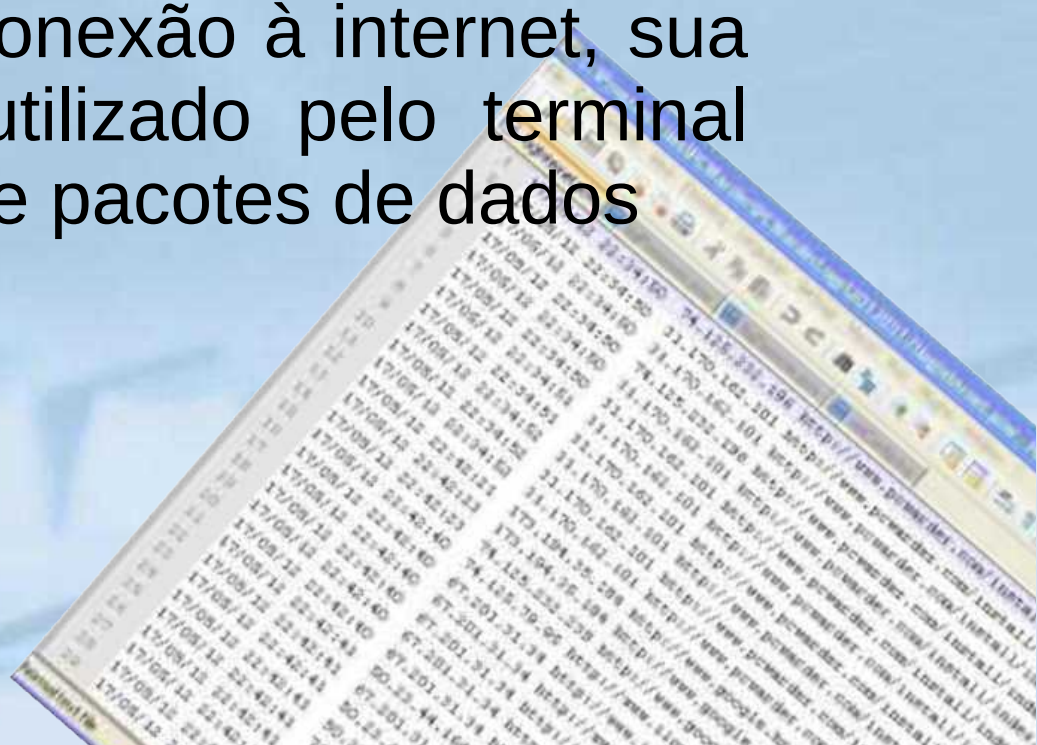
- Dos 23 artigos da lei Azeredo, 17 foram removidos;
- Na prática, a Lei Dieckmann restaura vários artigos que a Lei Azeredo perdeu, mas sem as *polêmicas do passado.
- Um diferencial ficou no Art. 4º da Lei Azeredo (LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012)
 - ***Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.***

E as polêmicas foram parar no...



publicada no Diário Oficial da União de 24/04/2014
*Estabelece princípios, garantias, direitos e deveres para o uso
da Internet no Brasil.*

- Guarda de registros de conexão e de acesso
 - Provedores de conexão à internet deverão manter armazenados pelo período de um ano, sob sigilo, em ambiente controlado e de segurança, conforme regulamento a ser editado, os registros de conexão de seus usuários;
- Conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados





- Guarda de registros de Aplicativos de Internet
 - Provedores de aplicações de internet deverão manter armazenados pelo período de seis meses, sob sigilo, em ambiente controlado e de segurança, conforme regulamento a ser editado, os respectivos registros de acesso a aplicações de internet;
- Conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.



Os referidos prazos de preservação dos registros poderão ser estendidos mediante requerimento cautelar de autoridade policial ou administrativa ou do Ministério Público (artigo 13).

Pedofilia

- Pedofilia é o desvio sexual caracterizado pela atração por crianças, com os quais os portadores dão vazão ao erotismo pela prática de obscenidades ou de atos libidinosos"
 - (Croce, 1995).



Imagens como esta, de **Martin Van Maele**, 1905, procuram ilustrar o distúrbio pedófilo.

Pedofilia

O termo "crime de pedofilia" é frequentemente utilizado de forma equivocada pelos meios de comunicação. A lei brasileira não possui o tipo penal "pedofilia". A pedofilia, como contato sexual entre crianças e adultos, se enquadra juridicamente no crime de **estupro de vulnerável (art. 217-A do Código Penal)** com pena de **oito a quinze anos** de reclusão e considerados crimes hediondos. Os meios de comunicação de forma insistente invocam como verdade a equiparação de uma condição psicológica com um ato criminoso.

Pornografia infantil

Pornografia infantil é crime no Brasil, passível de pena de prisão de dois a seis anos e multa. **Artigo 241, do Estatuto da Criança e do Adolescente (Lei nº 8.069/90)**: Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores (internet), fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

- Pena pode chegar a seis anos de cadeia mais multa;

Em novembro de 2003, a abrangência da lei aumentou, para incluir também a divulgação de links para endereços contendo pornografia infantil como crime de igual gravidade.

O Ministério Público do país mantém parceria com a **ONG SaferNet** que recebe denúncias de crimes contra os Direitos Humanos na Internet e mantém o sítio SaferNet, que visa a denúncia anônima de casos suspeitos de pornografia infantil na internet.

Na empresa, Privacidade?

A empresa têm a propriedade da estação de trabalho, do acesso à Internet e do e-mail corporativo

(seunome@nomedaempresa.com.br). Lhe é assegurado o direito à propriedade, pelo artigo 5º, da Constituição Federal, no inciso XXII: “é garantido o direito de propriedade”.

Na empresa, Privacidade?

A empresa tem o direito de proteger seu patrimônio, ainda, pelo Código Civil, artigo 1.228: “o proprietário tem a faculdade de usar, gozar e dispor da coisa, e o direito de reavê-la do poder de quem quer que injustamente a possua ou detenha” — o que quer dizer que, além de adquirir o bem, o indivíduo pode fazer o que quiser com o que tem e de reaver o que lhe for tirado.

Na empresa, Privacidade?

O Tribunal Superior do Trabalho, em decisão (TST - AIRR 613/2000), determinou que o empregador tem o direito de monitorar os e-mails corporativos e o acesso à internet por parte de seus empregados, entendendo, em suma, que a empresa é a proprietária dos instrumentos de trabalho utilizados para o acesso e de que o ambiente de trabalho não é um ambiente com expectativa de privacidade.



Desídia

- É a ociosidade, indolência, preguiça, desleixo. Constitui justa causa para rescisão do contrato de trabalho pelo empregador. A desídia, portanto, é falta de diligência do empregado em relação à execução dos serviços que lhe estão afetos. É caracterizada pela negligência, imperícia ou imprudência. Nota-se que a desídia não se confunde com o dolo (vontade de causar o dano).
 - Fundamentação:
 - Artigo 7º, inciso I, da Constituição Federal
 - Artigo 482, alínea “e”, da Consolidação das Leis do Trabalho

Escopo da Investigação e perícia

Esquema

Extrajudicial Judicial

Judiciário

Investigação extrajudicial

- Equipe interna
- Profissional externo
- Empresa externa



Pessoa Física



Pessoa Jurídica de Direito Privado



Pessoa Jurídica de Direito Público

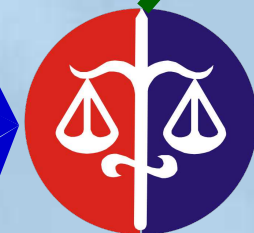
Sindicância

- Comissão de sindicância
- Corregedoria



Ação Judicial

- Perito Oficial
- Assistente Técnico



Ministério Público

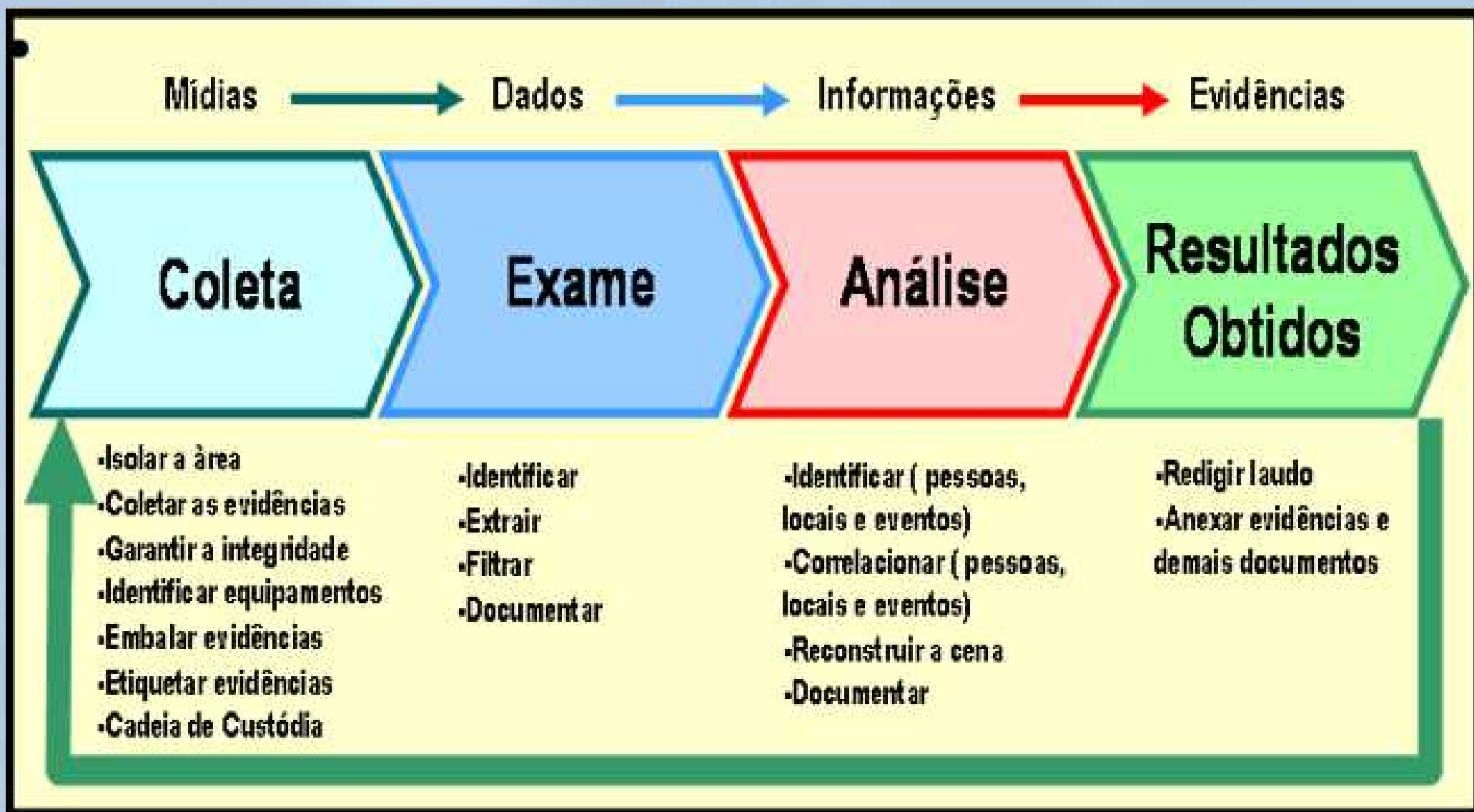


Polícia Judiciária (civil ou federal)

Inquérito Policial

- Investigador
- Perito Criminal
- Médico legista

Fases de um processo de Investigação



Probabilidade

- A probabilidade é a chance de uma falha de segurança ocorrer levando-se em conta o grau das vulnerabilidades presentes nos ativos que sustentam o negócio e o grau das ameaças que possam explorar estas vulnerabilidades.

Impacto

- O impacto de um incidente são as potenciais conseqüências que este incidente possa causar ao negócio da organização.

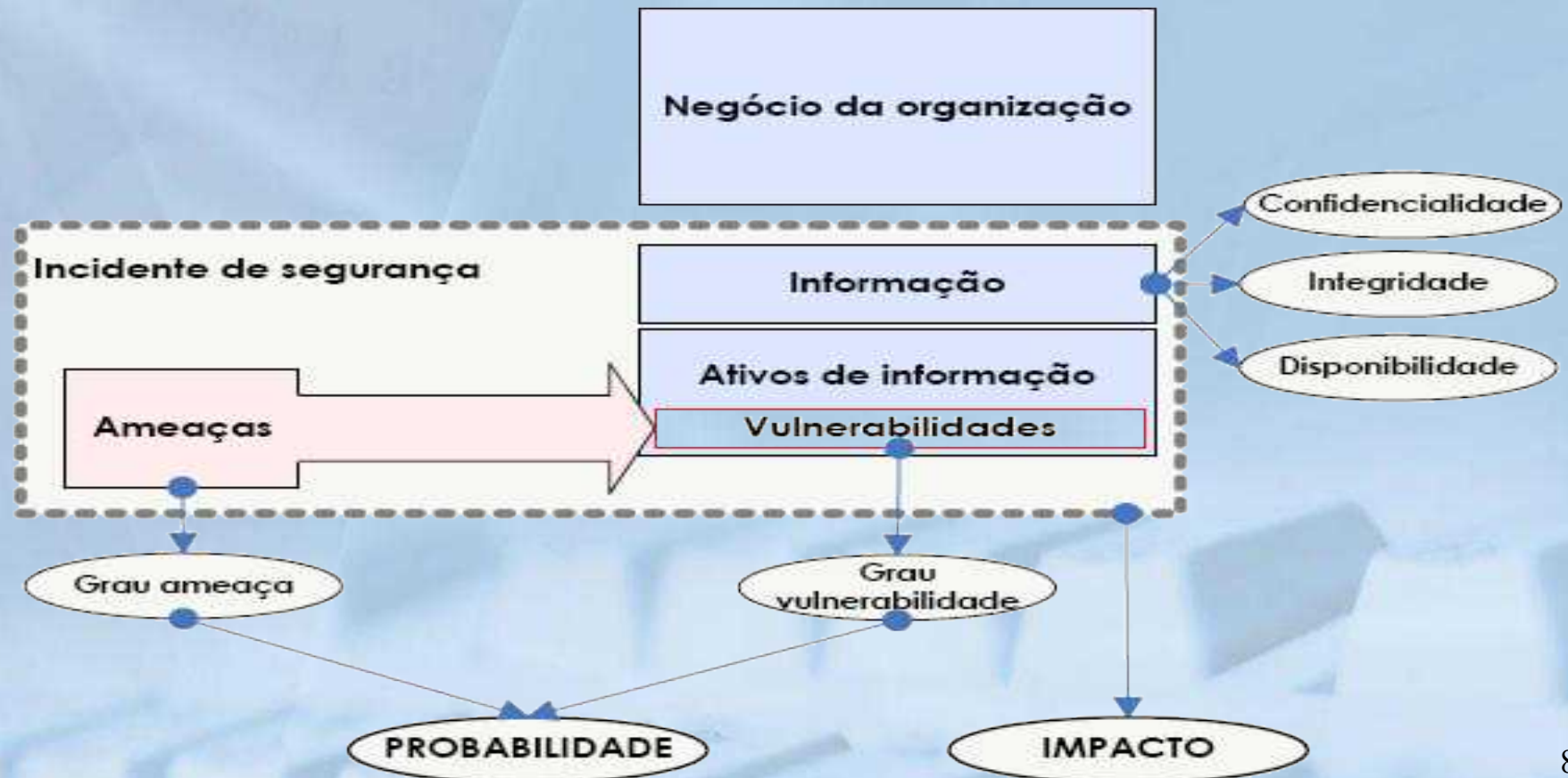
RISCO

- O risco é a relação entre a probabilidade e o impacto. É a base para a identificação dos pontos que demandam por investimentos em segurança da informação.

RISCO=IMPACTO*PROBABILIDADE

Incidente de Segurança da Informação

- Quando uma ameaça explora vulnerabilidades de um ativo de informação, violando uma de suas características de segurança (CID), temos o incidente de segurança da informação. Este incidente tem uma chance de acontecer, e se acontecer gera um determinado impacto ou prejuízo.



Segurança

- As ameaças são crescentes, e atualmente miram o fator humano
- A segurança pode ser estabelecida em diferentes níveis, com diversos controles
- A aplicação de medidas de proteção deve ser feita de forma responsável, alinhada com o negócio, mediante avaliação de riscos
- A documentação é fundamental, e deve ser retransmitida ao usuário para que ele saiba que a segurança também depende dele
- Parafraseando Bruce Schneier: “A segurança não é um produto, é um processo”

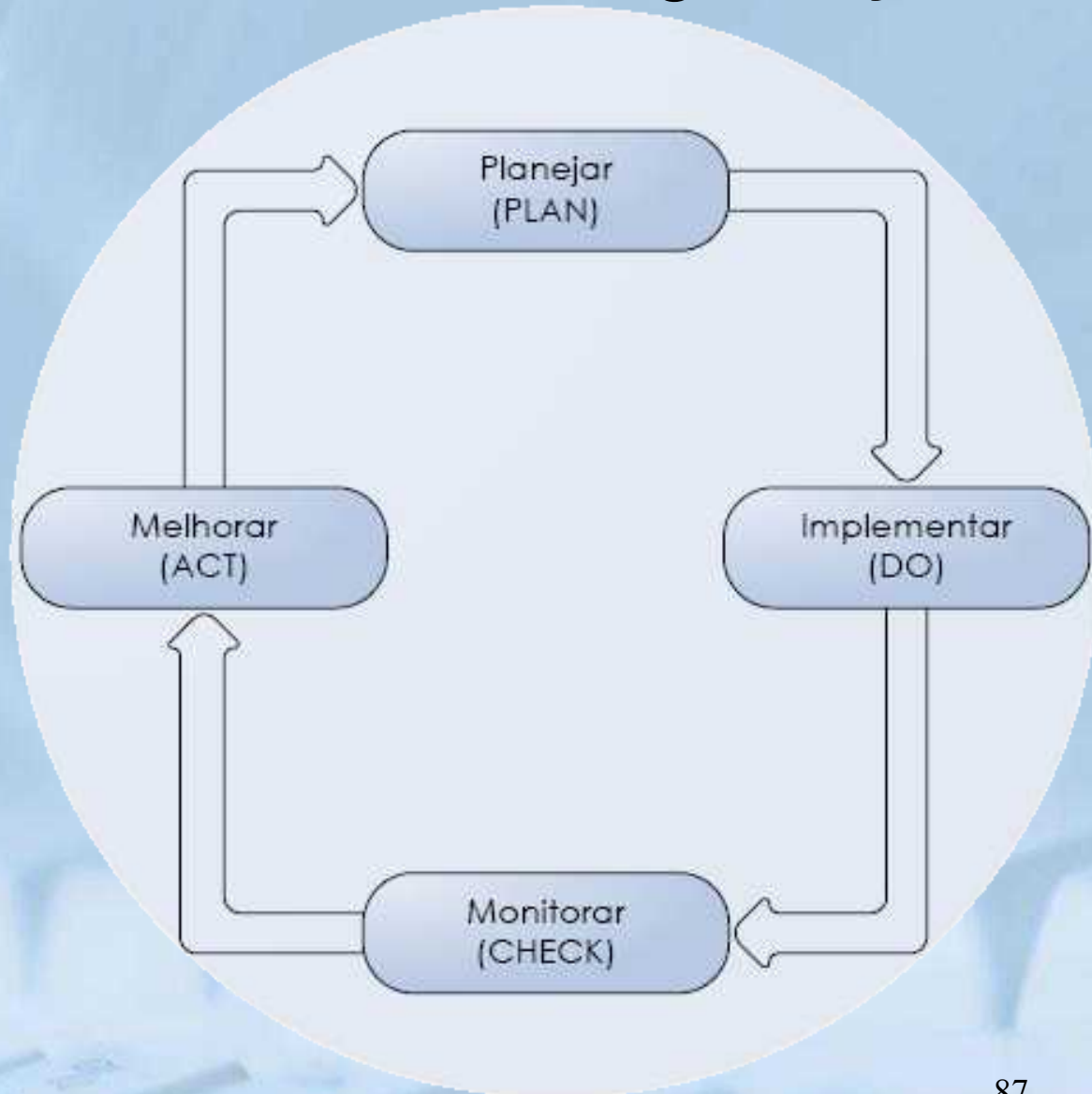
Como implementar um sistema de segurança

- Conhecer os conceitos sobre segurança da informação não significa necessariamente saber garantir esta segurança. Muitos têm experimentado esta sensação quando elaboram seus planos de segurança e acabam não atingindo os resultados desejados.

- Um gerente de segurança da informação de verdade trabalha com fatos, com resultados de análise e exames da organização em questão.
 - A partir destes resultados ele estabelece um conjunto de ações coordenadas no sentido de garantir a segurança da informação; um conjunto de ações, um conjunto de mecanismos integrados entre si, de fato, um sistema de segurança da informação.

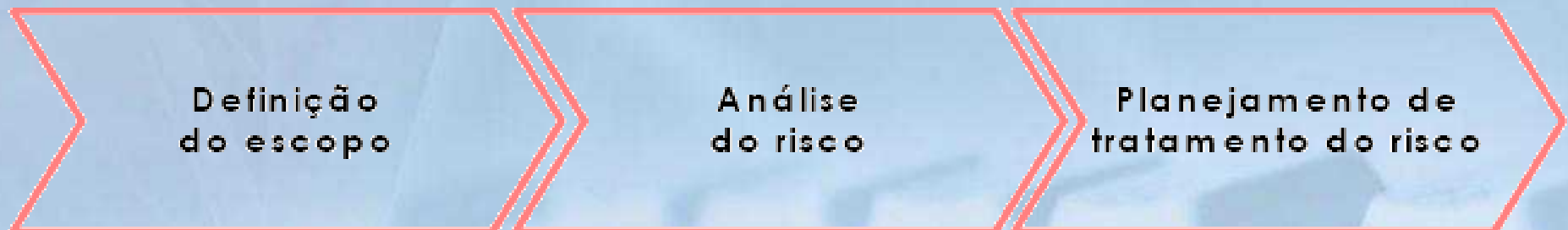
Como implementar um sistema de segurança

- A implantação de um sistema de segurança da informação não é uma tarefa trivial.
- O modelo proposto pela Qualidade (família ISO) é o caminho adequado superar este desafio. Este modelo é baseado no conceito de melhoria contínua (PDCA).



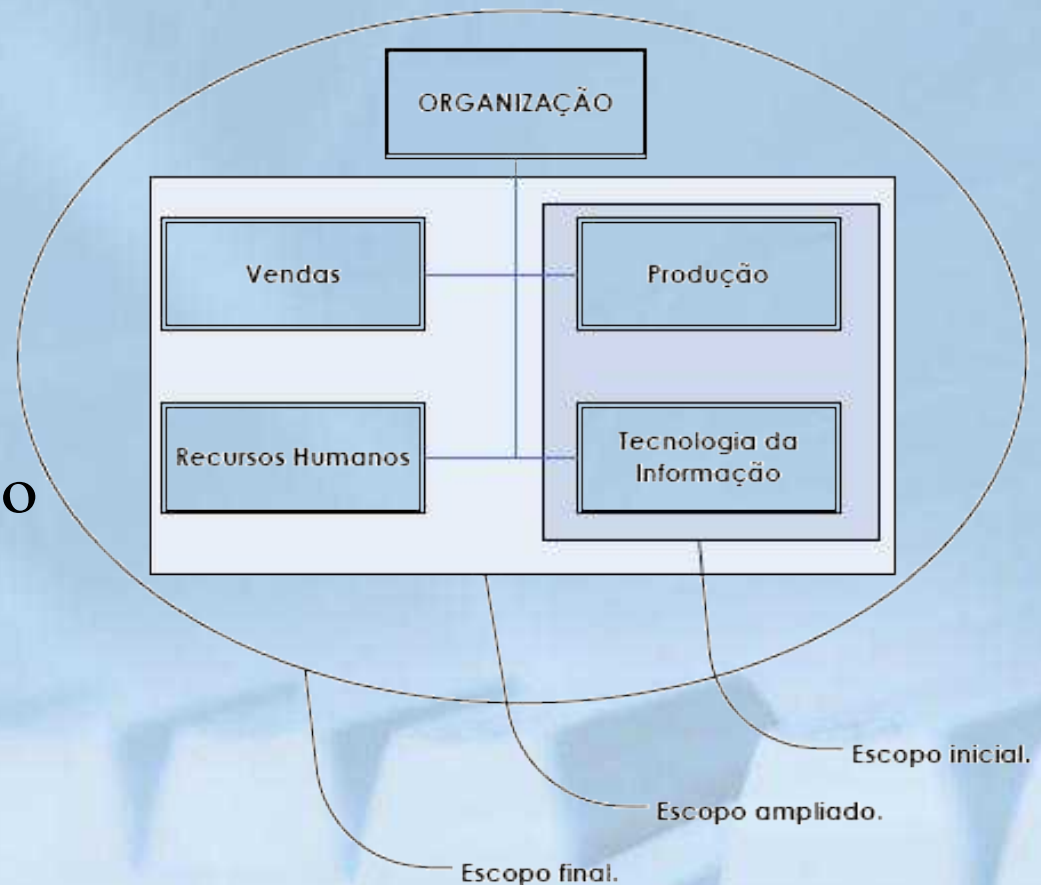
Como implementar um sistema de segurança

- A primeira fase é de planejamento (PLAN). Nesta fase, é definido o escopo e abrangência esperada para o sistema de segurança da informação, e realizada a análise de risco, e feito o planejamento para o tratamento do risco.



Como implementar um sistema de segurança

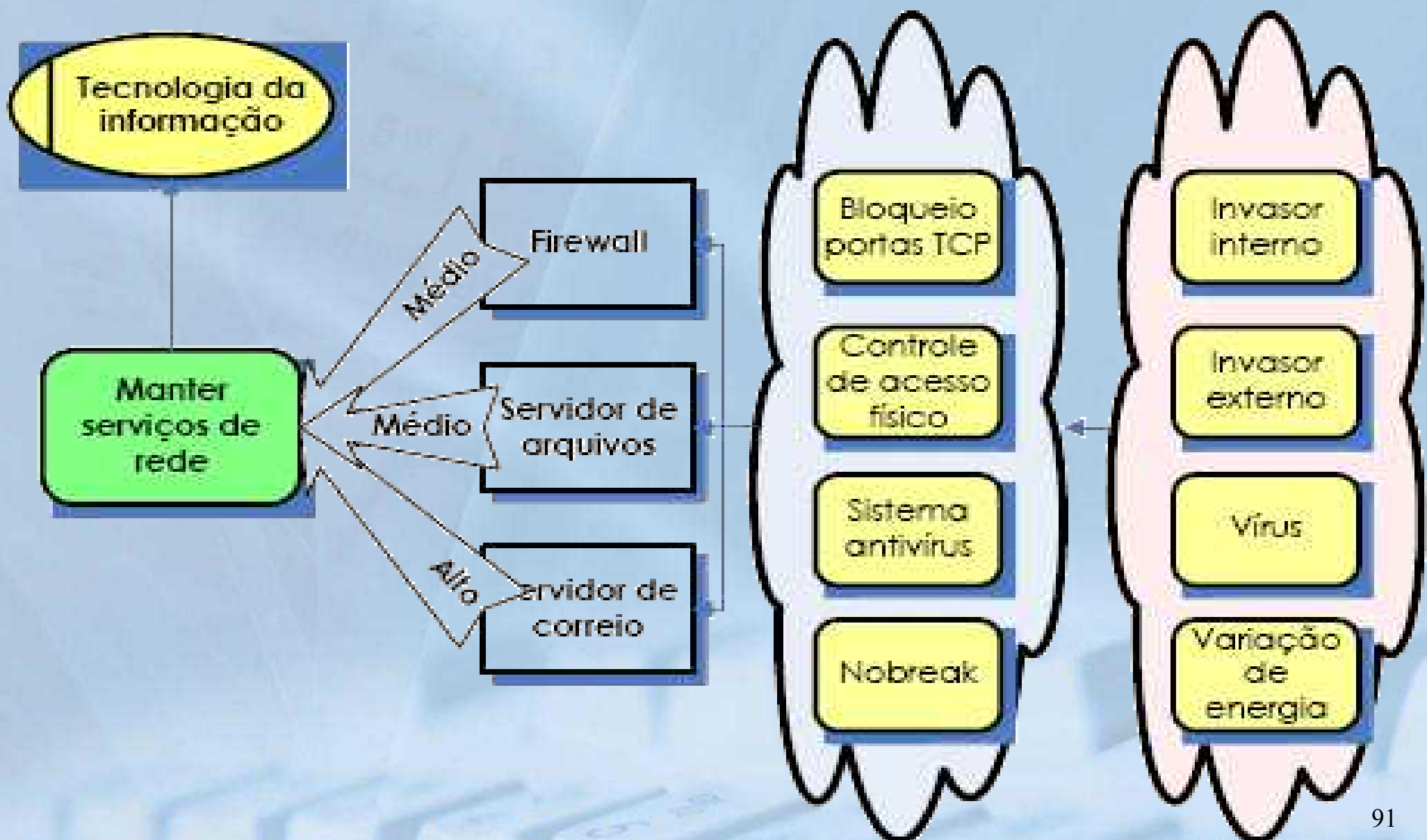
- Escopo
 - Nem sempre é fácil implantar o sistema em toda a organização. Por isso, definir escopos sucessivamente maiores talvez seja o caminho para se chegar ao objetivo final: segurança da informação em toda a organização.



Análise de risco

- Depois do escopo definido, é a hora de pensar que controles implementar.
 - Para otimizar esta decisão é imprescindível realizar a análise de risco. Ela apontará para as prioridades dentro do escopo.
 - A análise deve ser feita considerando as seguintes dimensões: processos, tecnológica, ambiental, e pessoas.

Análise de risco



Análise de risco

120	Ativo	Impacto	Incidente	Dias/Ano	Ocorrências	Vulnerabilidade	GV	Ameaça	GE	Probabilidade	RISCO
Manter serviços de rede	Firewall	50,00%	Invasão	3	0,82%	Portas TPC abertas	80,00%	Invasor externo (hacker)	100,00%	90,00%	46,94%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	28,33%
			Contaminação por vírus	15	4,11%	Sem sistema antivírus	10,00%	Vírus	100,00%	55,00%	36,37%
			Queda de energia	36	9,86%	Sem nobreak	10,00%	Variação de energia	50,00%	30,00%	29,95%
	Servidor de arquivos	55,00%	Invasão	0	0,00%	Portas TPC abertas	5,00%	Invasor externo (hacker)	30,00%	17,50%	24,17%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	30,00%
			Contaminação por vírus	0	0,00%	Sem sistema antivírus	10,00%	Vírus	80,00%	45,00%	33,33%
			Queda de energia	0	0,00%	Sem nobreak	10,00%	Variação de energia	50,00%	30,00%	28,33%
	Servidor de correio	75,00%	Invasão	0	0,00%	Portas TPC abertas	50,00%	Invasor externo (hacker)	30,00%	40,00%	38,33%
				0	0,00%	Sem controle de acesso físico	60,00%	Invasor interno	10,00%	35,00%	36,67%
			Contaminação por vírus	0	0,00%	Sem sistema antivírus	10,00%	Vírus	80,00%	45,00%	40,00%

Análise de risco

- tecnologias, ambientes e pessoas são, de fato, ativos de informação; ou categorizações destes ativos.
- As pessoas ocupam uma posição central entre estas categorias, pois sua importância é maior do que a das outras.

O que fazer com o risco?

- Com o risco já identificado, é importante decidir o que fazer com ele.
- É possível:
 - Evitar
 - Controlar
 - Transferir
 - Aceitar

Declaração de aplicabilidade

Controle	Item da ISO	Objetivo	Justificativa	Prioridade da análise de risco
Fórum de segurança da informação	4.1.1	Aprovar as ações em segurança		MÁXIMA
Comitê coordenador de segurança da informação	4.1.2	Contribuir com a implantação das ações		MÁXIMA
Definição de responsabilidades sobre segurança da informação	4.1.3	Garantir o comprometimento com a segurança		MÉDIA
Autorização para aquisição de processadores de informação	4.1.4	Garantir o controle dos ativos de segurança		MÉDIA
Consultoria especializada em segurança da informação	4.1.5	Não será implementado.	A organização investiu em recursos internos.	MÍNIMA
Cooperação entre organizações	4.1.6	Gestão de conhecimento sobre segurança		IGNORADO
Revisão de segurança da informação independente	4.1.7	Garantir a qualidade do sistema de segurança da informação da organização		IGNORADO
Identificação de risco do acesso de terceirizados	4.2.1	Controlar as informações que são acessadas		ALTA
Requisitos de segurança em contratos de terceirização	4.2.2	Garantir a segurança da informação na relação com terceiros através da assinatura de contratos		ALTA
Requisitos de segurança em contratos de <i>outsourcing</i>	4.3.1	Garantir a segurança da informação na relação com terceiros através da assinatura de contratos		ALTA

Implementando o sistema

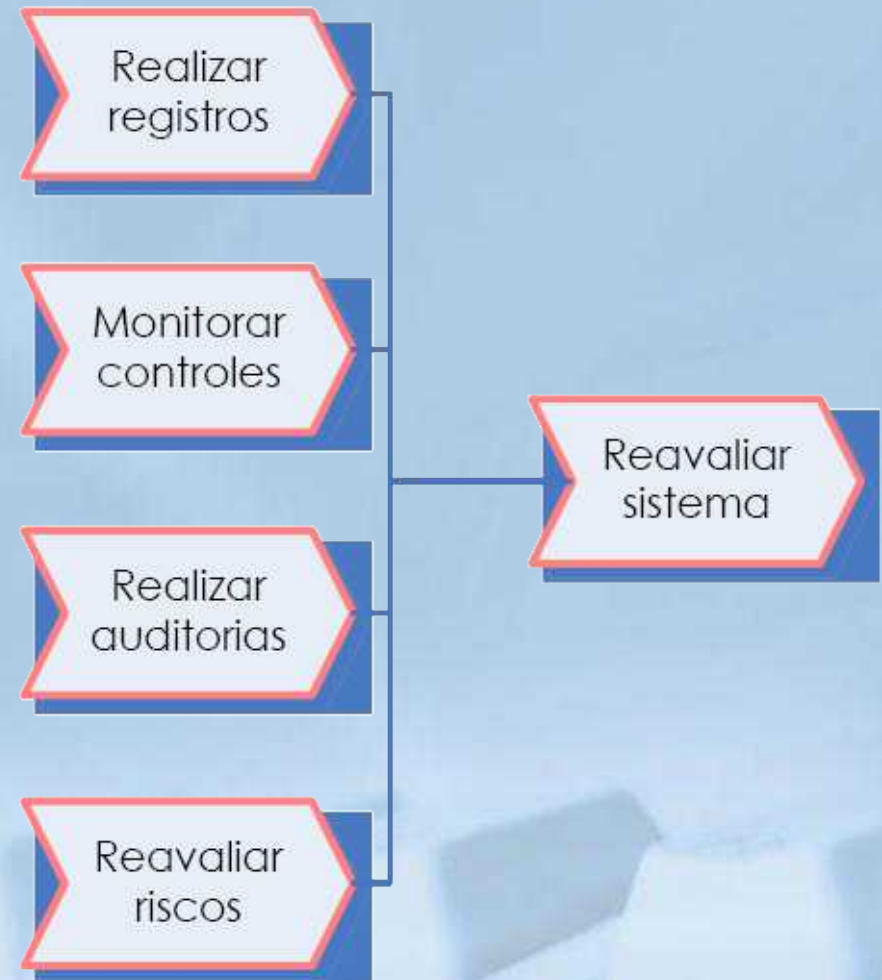
- Após a etapa de planejamento, o próximo passo é executar o planejado. Isto envolve o planejamento da fase de implementação, a execução e o controle da implementação, e por fim, o encerramento da implementação.



Monitorando o sistema de segurança

O monitoramento ou controle do sistema implica em avaliar sistematicamente se os controles implementados estão atendendo as expectativas originais. Para tanto, os processos ao lado precisam ser executados com regularidade.

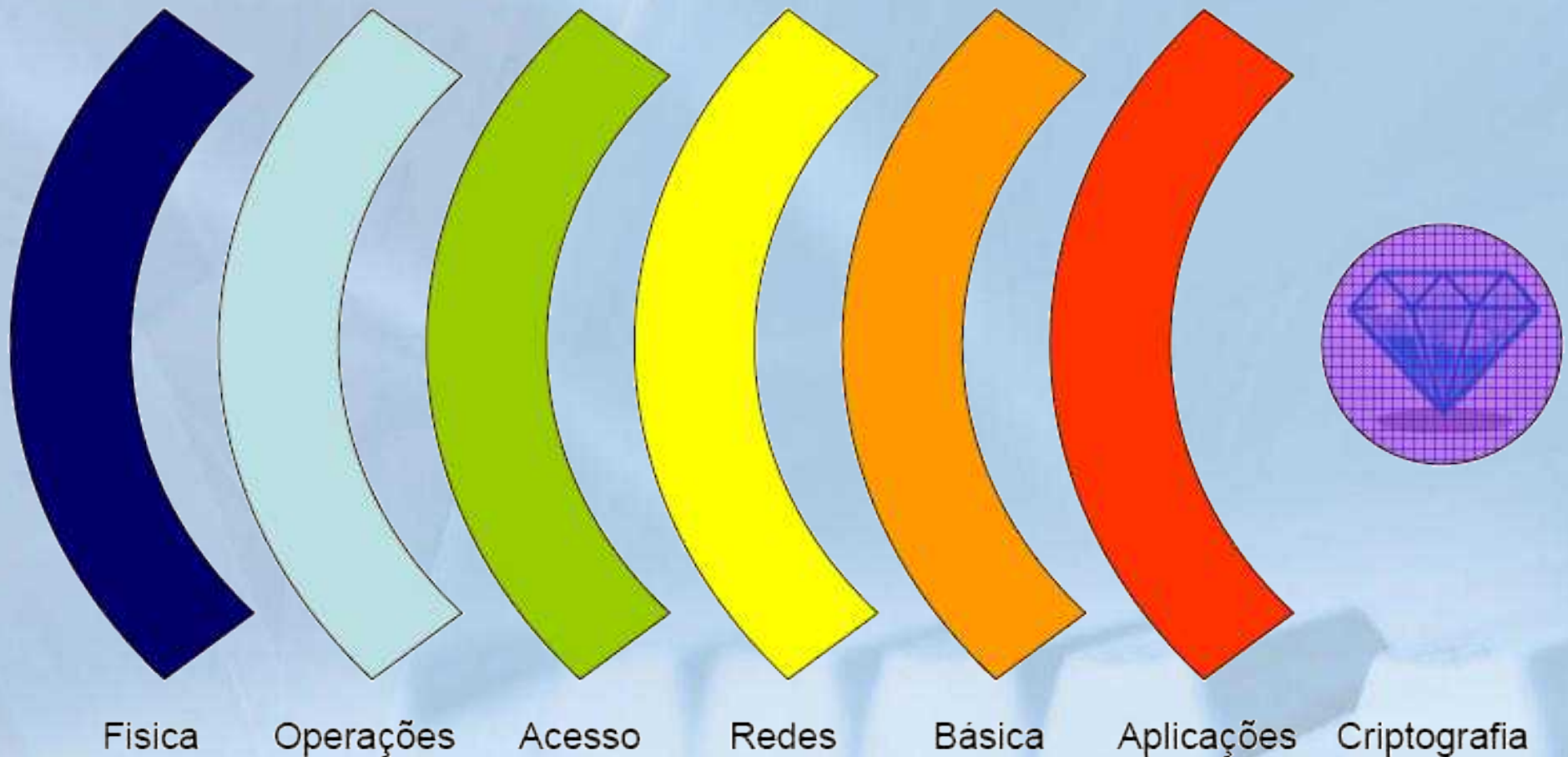
registros



Controles de segurança da informação

- A implementação de um sistema de segurança da informação se dá pela instalação de controles específicos nas mais diversas áreas da organização, sempre pensando nas dimensões de processos, tecnologias, ambientes e pessoas.

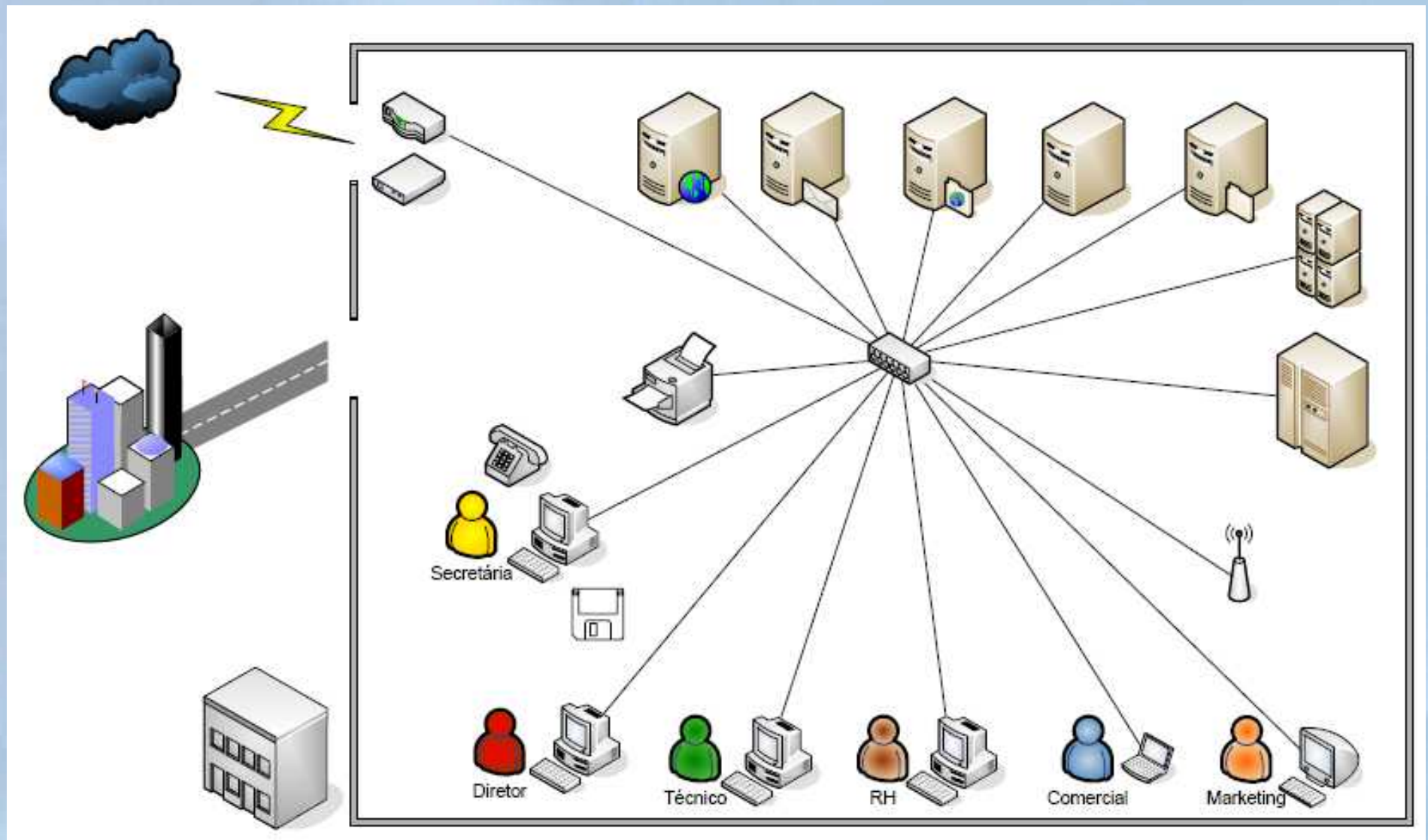
Camadas de proteção: controles



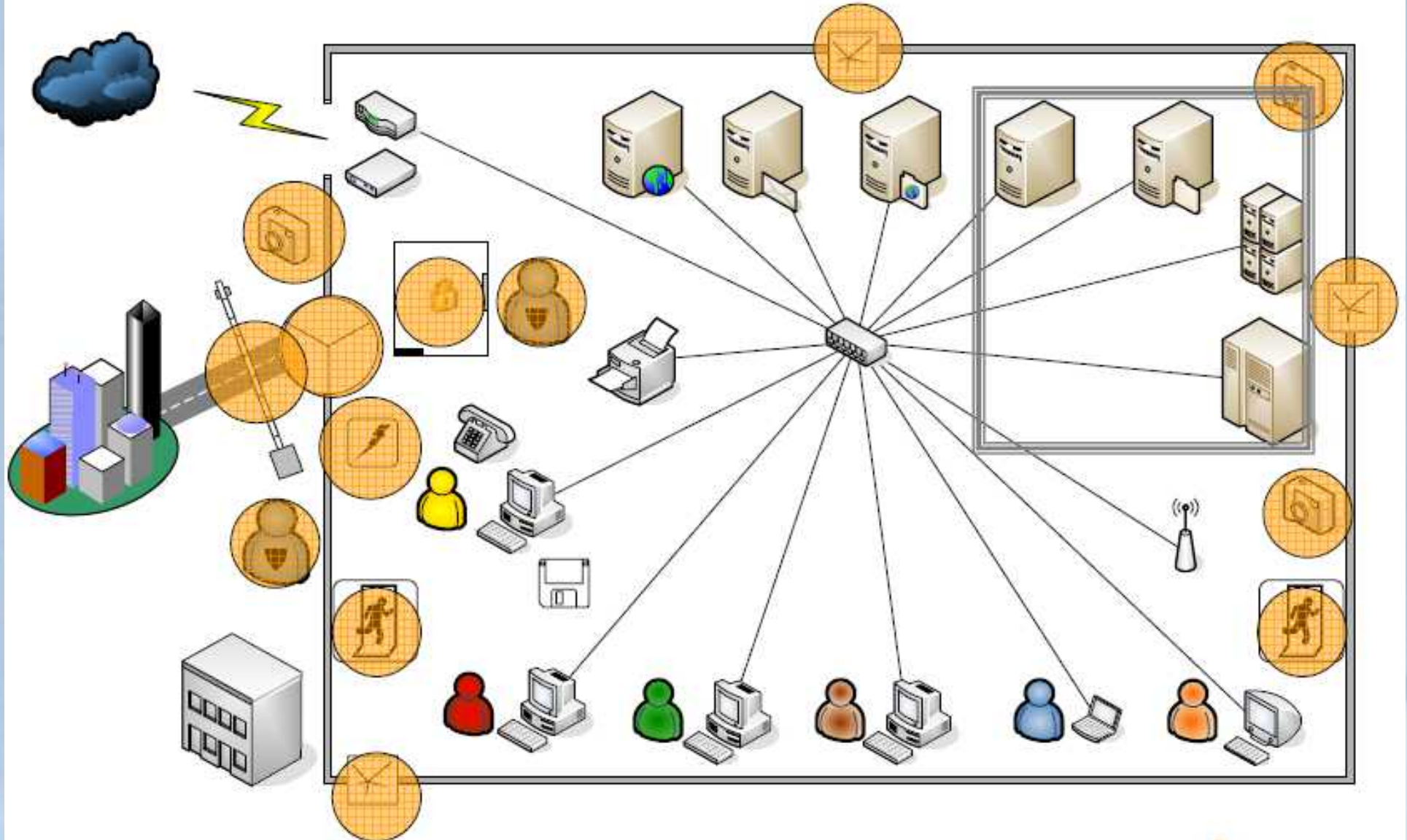
Segurança Física

- Cercas/ portões
- Portas/ portarias
 - Catracas
 - Detectores de metais
 - Crachás
- Paredes/ janelas
 - Sensores de invasão
- Seguranças
- CFTV
- Sistema de climatização
- Documentação de elementos de engenharia civil/ elétrica/ hidráulica
- Sistema de detecção/ combate a incêndio
- Compartimentalização de ambientes

Como acontece



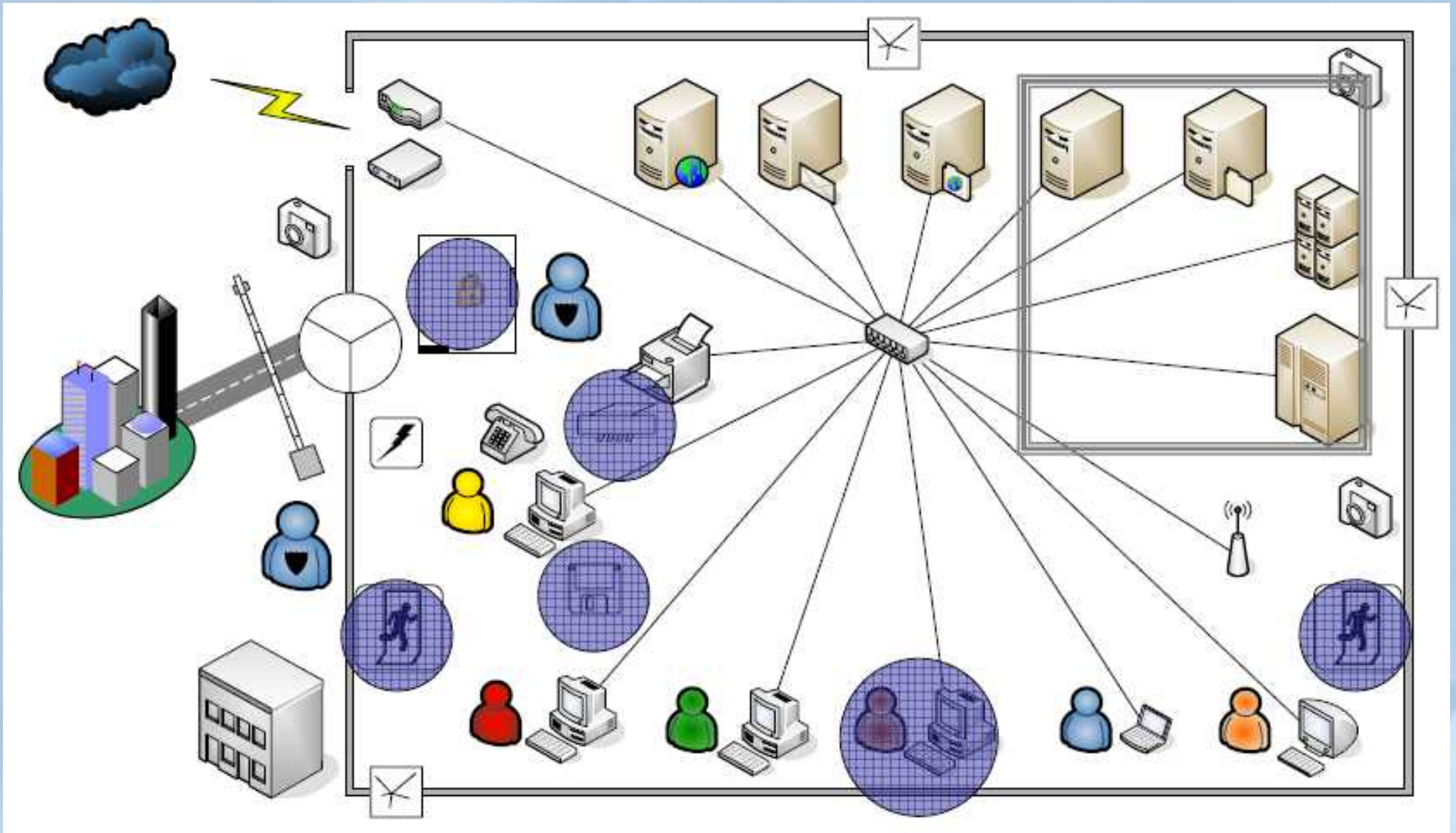
Como deveria acontecer



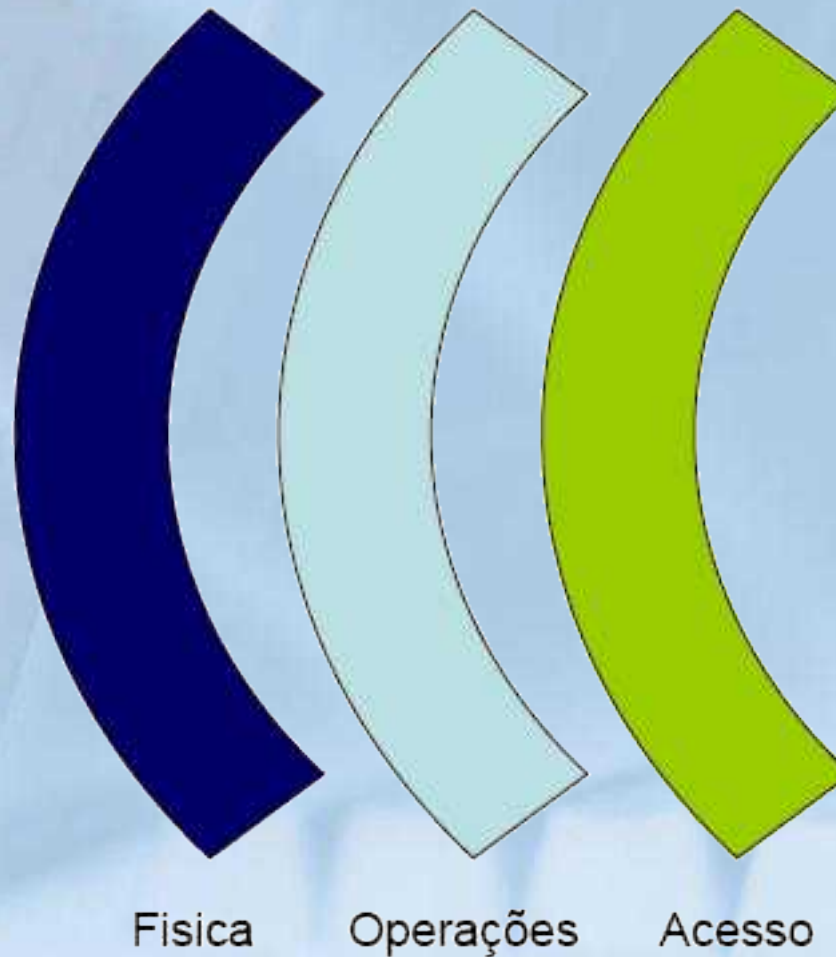
Segurança de Operações

- Controles
 - Hardware e equipamentos
 - Software
 - Pessoal (Gestão de RH)
- Manejo de mídia
 - Armazenamento
 - Descarte
- Mesas e quadros limpos
- CSIRT (Computer Security Incident Response Team)
- Mecanismos de controle e verificação
 - Recuperação de Desastres
 - Análises de vulnerabilidades/ testes de invasão
 - Controle de logs

Segurança de Operações



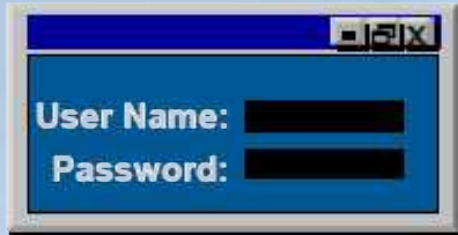
Controle de Acesso



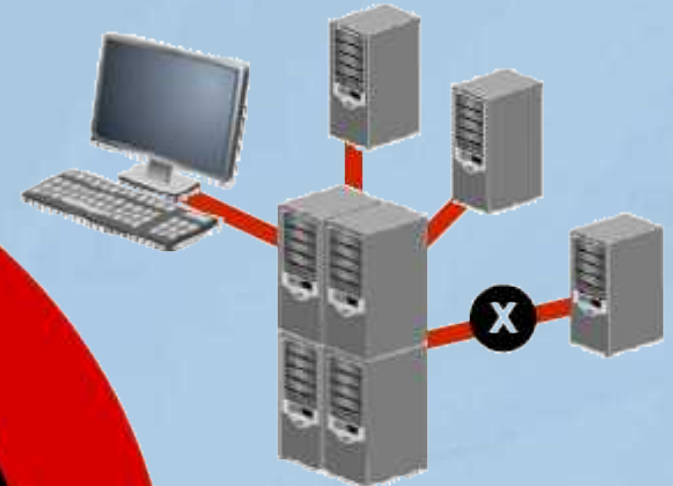
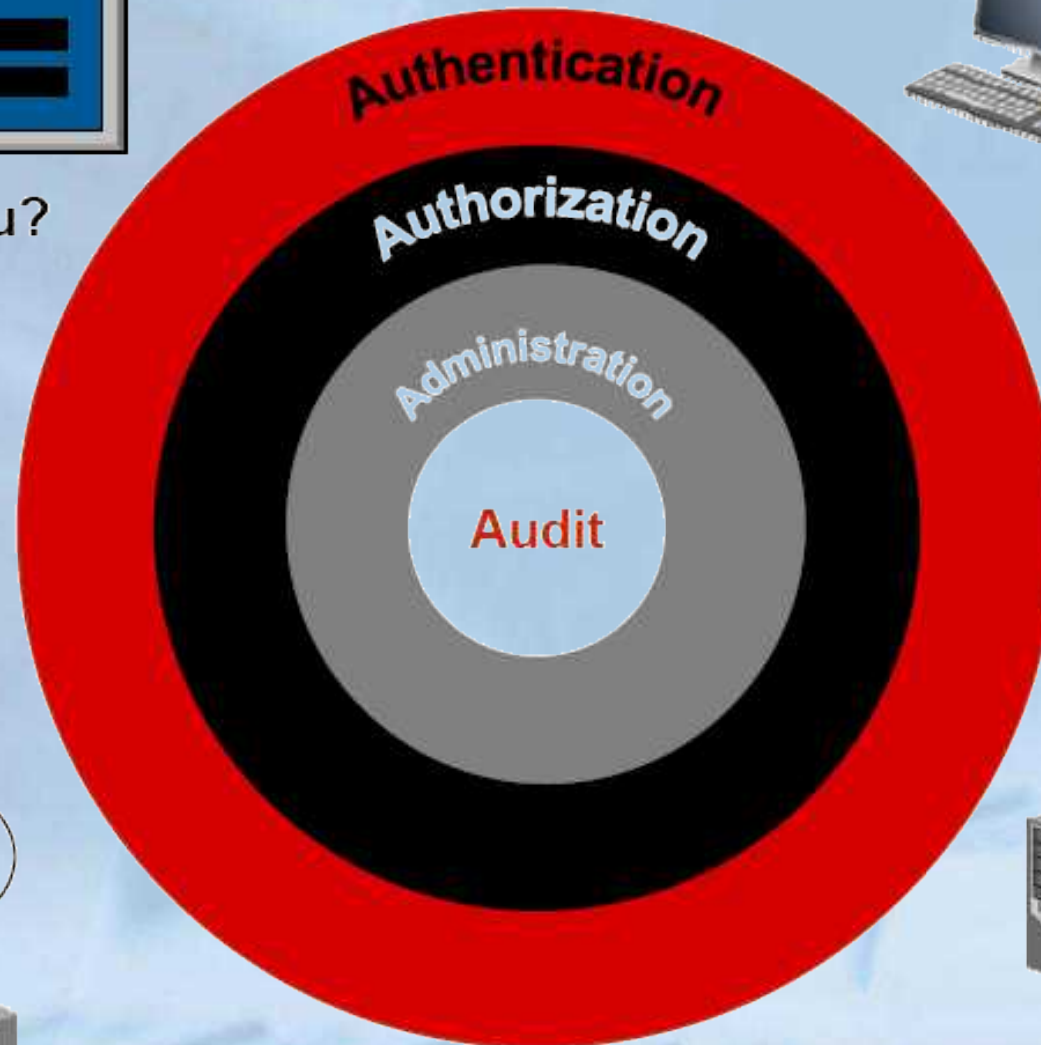
Controle de Acesso

- Ambientes
 - Biometria
 - Crachás
- Sistemas
 - ACLs
 - Biometria, tokens, smartcards, etc
 - SSO
 - Serviços de autenticação AAA (ex. RADIUS)
- Os mecanismos de autenticação de usuários dividem-se em três categorias:
 - baseados no conhecimento
 - (o que se sabe)
 - baseados em propriedade
 - (o que se possui)
 - baseados em características
 - (o que se é)

O AAAA da segurança

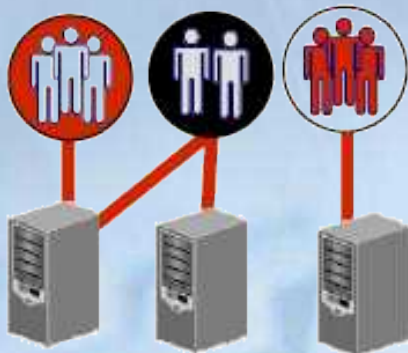


Who are you?



What can you do?

How do we
manage all
of this...?



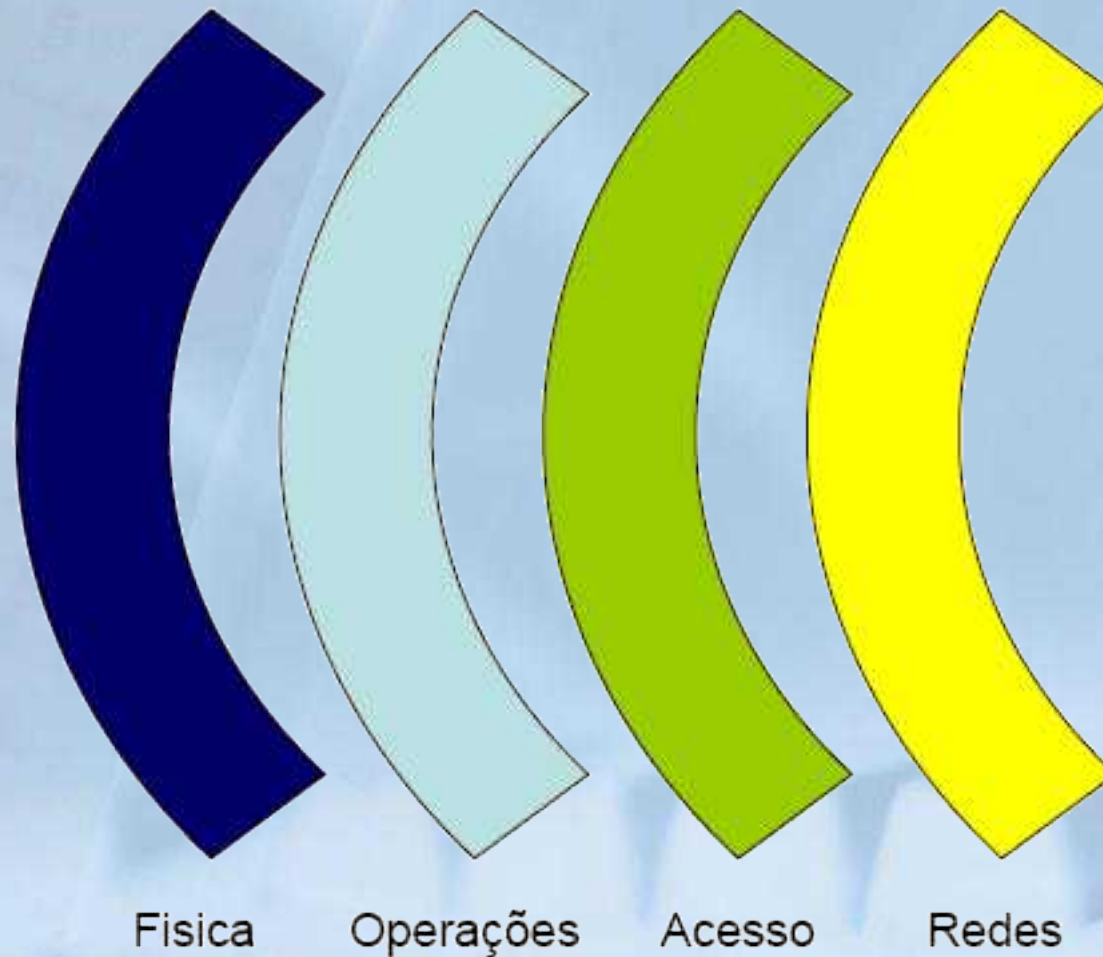
What has
actually
happened?



Fraquezas das senhas

- Pessoas podem escolher senhas fracas, fáceis de adivinhar;
- Quando escolhem (ou são obrigadas a usar) senhas fortes, escrevem em um papel de fácil acesso;
- As senhas podem ser compartilhadas de forma indevida;
- Podem ser interceptadas, quando enviadas de forma desprotegida;
- Uma senha pode ser descoberta sem que o proprietário saiba;

Segurança de redes



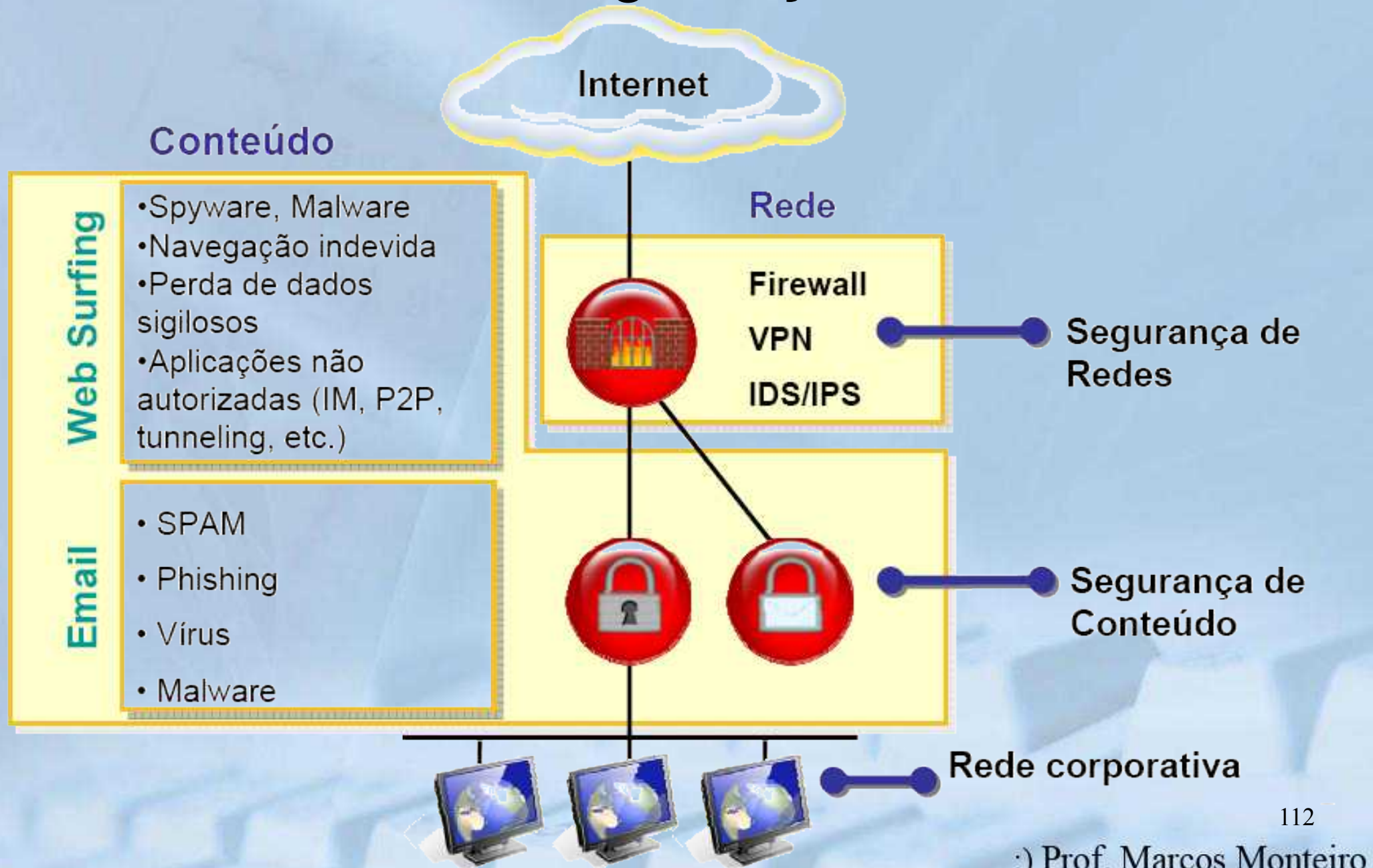
Segurança de redes

- Arquitetura
 - Segmentação de rede
 - DMZ
 - Honey Nets
 - Segregação de serviços e máquinas
- Controles
 - Firewall
 - IDS / IPS
 - Controle de banda
- Gerência de conteúdo
 - VPN criptografada
 - 802.1X
- Extras
 - Redundância de link
 - Balanceamento de carga

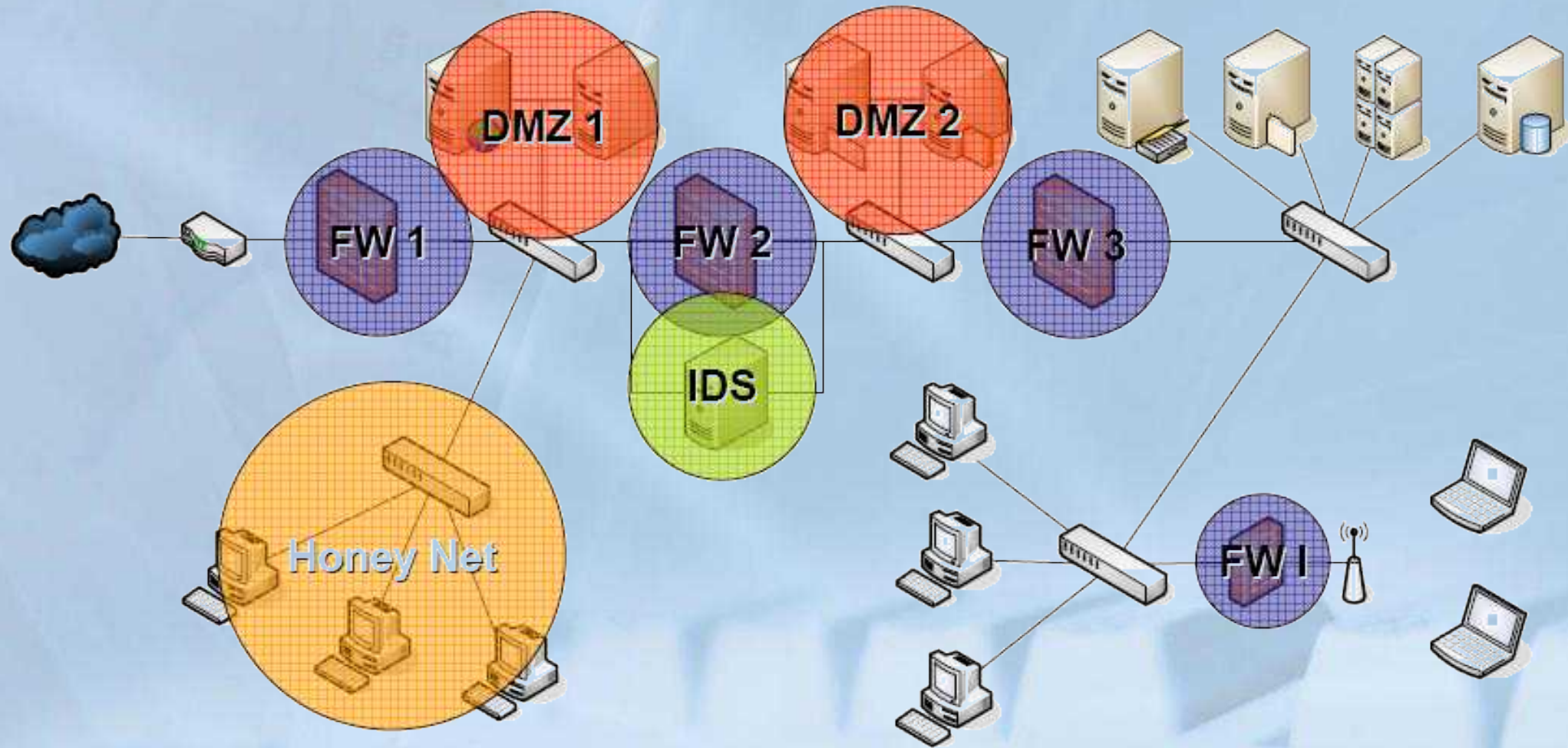
Objetivos da Segurança de Redes

- Estabelecer protocolos seguros que garantam
 - Confidencialidade (usando criptografia)
 - Integridade (através de verificações matemáticas)
 - Disponibilidade (introduzindo medidas que inibam ataques de DoS)
- O ponto crucial para alcançar a confidencialidade e a integridade é a autenticação
 - Acesso a sistemas devem ser permitidos somente a usuários autorizados

Elementos de Segurança de Perímetro



Topologia segura



Arquitetura de Segurança



Arquitetura de Segurança





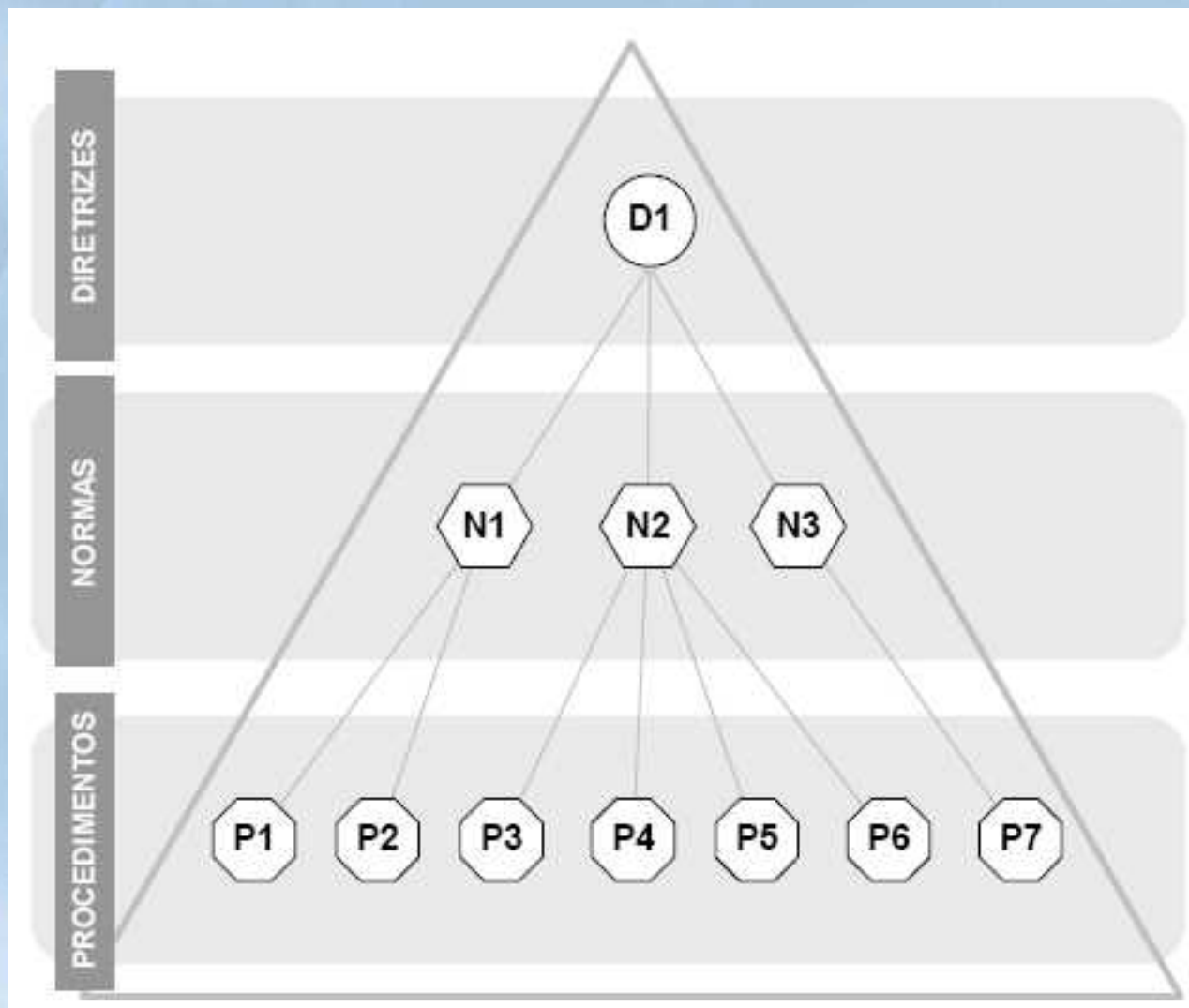
- Última linha de defesa
- Proteção de dados
 - ⇒ Em repouso
 - ⇒ Em trânsito
- Segurança de comunicações
 - ⇒ IPSec
 - ⇒ SSL
 - ⇒ Camadas 1 e 2

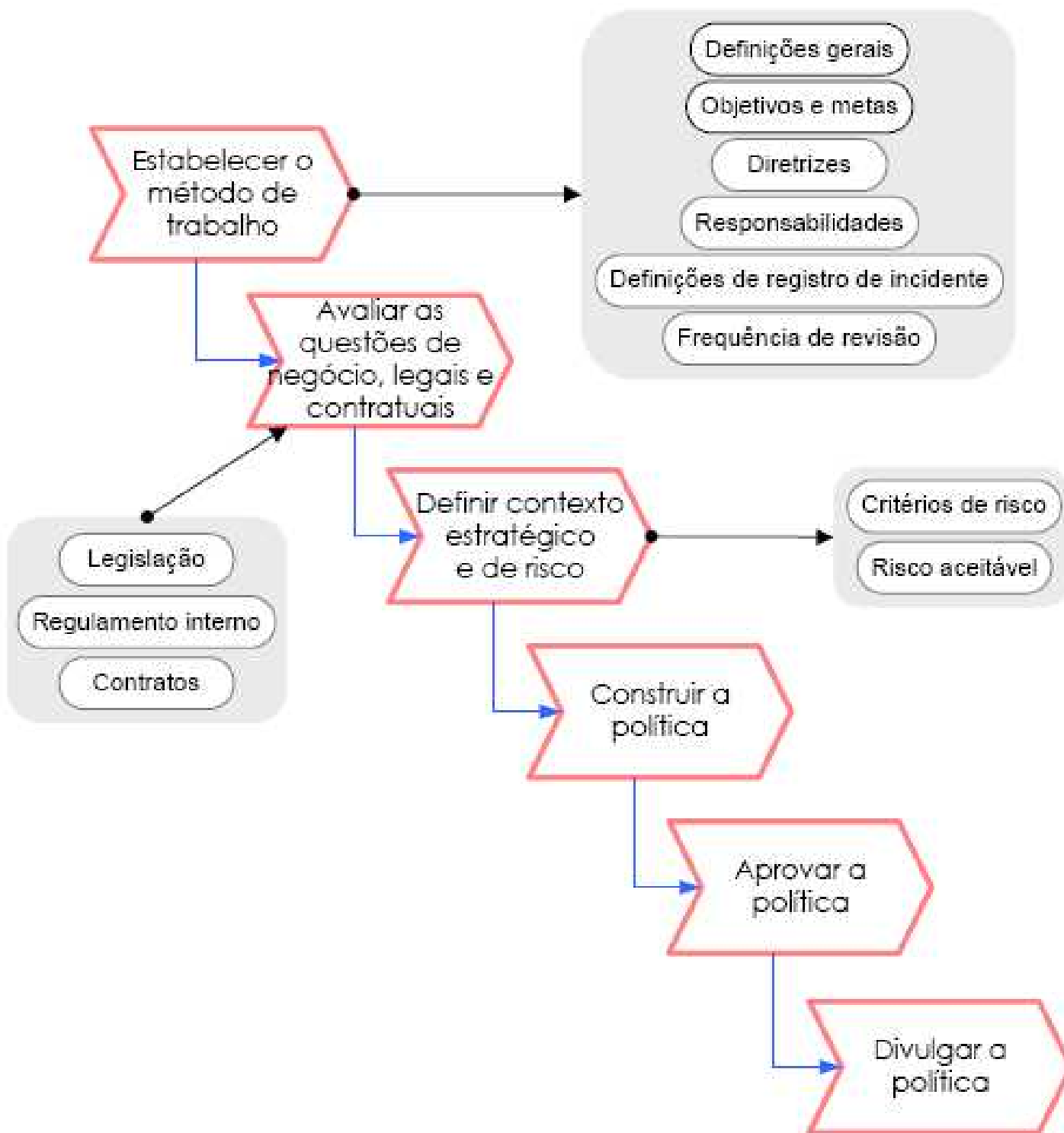


Política

A política de segurança da informação (PSI) deve estar alinhada com os objetivos de negócio da organização.

Ela é estruturada em diretrizes, normas e procedimentos.





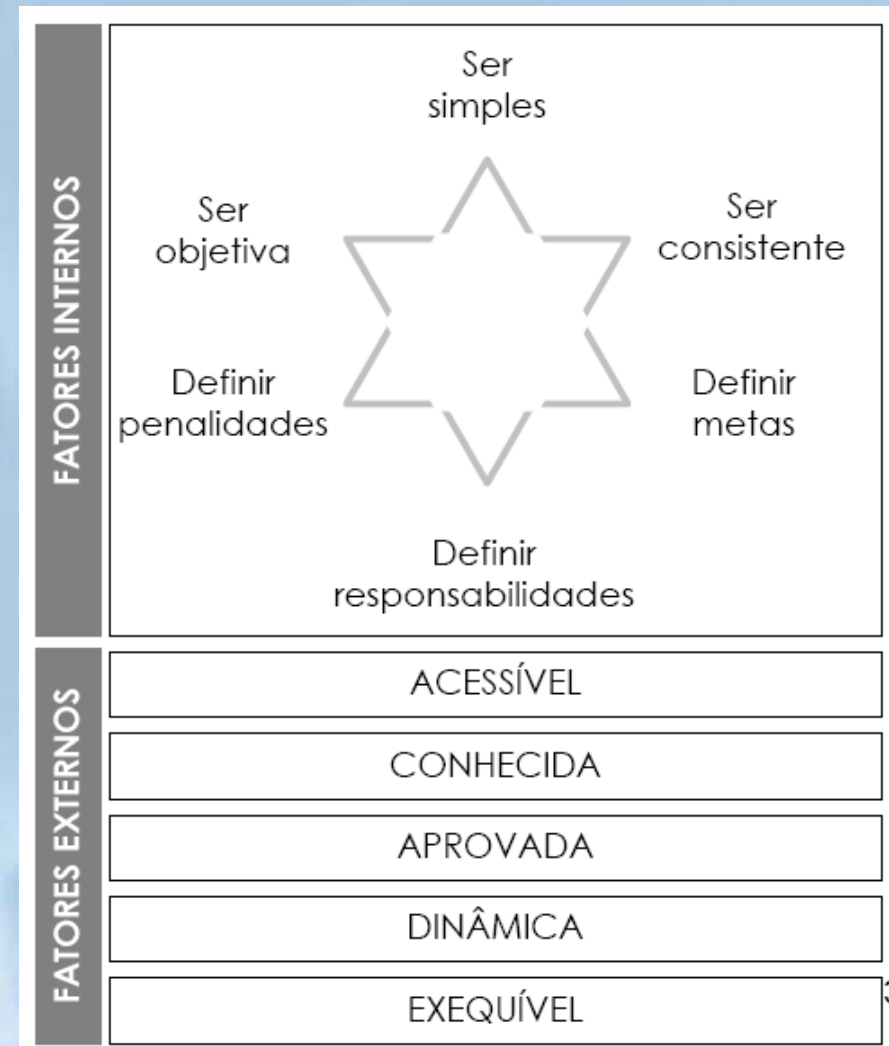
A elaboração e implantação de uma política de segurança é sem si mesmo um projeto a ser gerido.

Os passos essenciais são demonstrados na figura ao lado.

O governo federal está obrigado por decreto a possuir e respeitar uma política de segurança, conforme Decreto 3.505 de 13 de junho de 2000.

Política

A política possui características, ou fatores, internos e externos, que precisam ser respeitados por ocasião de sua elaboração e implantação.



Sistema de Gestão de Segurança da Informação

5. Política de Segurança

- 5.1. Política de Segurança da Informação
- 5.1.1 Documento da Política
- 5.1.2 Análise Crítica da Política

6. Organizando a Segurança

- 6.1. Infra-estrutura de Segurança
 - 6.1.1 Comprometimento da Direção
 - 6.1.2 Coordenação da Segurança
 - 6.1.3 Atribuição de Responsabilidades
 - 6.1.4 Processo Autorização de Recursos
 - 6.1.5 Acordos de Confidencialidade
 - 6.1.6 Contato com Autoridades
 - 6.1.7 Contato com grupos especiais
 - 6.1.8 Análise crítica independente da segurança da informação

6. Organizando a Segurança

- 6.2 Partes Externas
 - 6.2.1 Identificando riscos relacionados com partes externas
 - 6.2.2 Identificando segurança da informação com os clientes
 - 6.2.3 Identificando segurança da informação com os terceiros

7. Gestão de Ativos

- 7.1 Responsabilidade pelos Ativos
 - 7.1.1 Inventário dos Ativos
 - 7.1.2 Proprietário dos Ativos
 - 7.1.3 Uso aceitável dos Ativos

7. Gestão de Ativos

- 7.2 Classificação da Informação
- 7.2.1 Recomendações para classificação
- 7.2.2 Rótulos e tratamento da informação

8. Segurança dos Recursos Humanos

- 8.1 Antes da Contratação
 - 8.1.1 Papéis e responsabilidades
 - 8.1.2 Seleção
 - 8.1.3 Termos e condições de contratação

8. Segurança da Recursos Humanos

- 8.2 Durante a Contratação
 - 8.2.1 Responsabilidade da Direção
 - 8.2.2 Conscientização, educação e treinamento em segurança da informação
 - 8.2.3 Processo Disciplinar

8. Segurança da Recursos Humanos

- 8.3. Encerramento ou mudança da contratação
- 8.3.1 Encerramento de Atividades
- 8.3.2 Devolução de Ativos
- 8.3.3 Retirada de direitos de acesso

9. Segurança Física e do Ambiente

- 9.1. Áreas Seguras
 - 9.1.1 Perímetro de Segurança Física
 - 9.1.2 Controles de entrada física
 - 9.1.3 Segurança em escritórios, salas e instalações
 - 9.1.4 Proteção contra ameaças externas e do meio ambiente
 - 9.1.5 Trabalhando em áreas seguras
 - 9.1.6 Acesso do público, áreas de entrega e de carregamento

9. Segurança Física e do Ambiente

- 9.2. Segurança de Equipamentos
 - 9.2.1 Instalação e proteção do equipamento
 - 9.2.2 Utilidades
 - 9.2.3 Segurança do Cabeamento
 - 9.2.4 Manutenção dos equipamentos
 - 9.2.5 Segurança de equipamentos fora das dependências da organização
 - 9.2.6 Reutilização e alienação segura de equipamentos
 - 9.2.7 Remoção de propriedade

10. Gerenciamento das Operações e Comunicações

- 10.1 Procedimentos e responsabilidade operacionais
 - 10.1.1 Documentação dos procedimentos de operação
 - 10.1.2 Gestão de mudanças
 - 10.1.3 Segregação de funções
 - 10.1.4 Separação dos recursos de desenvolvimento, teste e de produção

10. Gerenciamento das Operações e Comunicações

- 10.2. Gerenciamento de serviços terceirizados
 - 10.2.1 Entrega de serviços
 - 10.2.2 Monitoramento e análise crítica de serviços terceirizados
 - 10.2.3 Gerenciamento de mudanças para serviços terceirizados

10. Gerenciamento das Operações e Comunicações

- 10.3 Planejamento e aceitação dos sistemas
- 10.3.1 Gestão de capacidade
- 10.3.2 Aceitação de sistemas

10. Gerenciamento das Operações e Comunicações

- 10.4. Proteção contra códigos maliciosos e códigos móveis
- 10.4.1 Controles contra códigos maliciosos
- 10.4.2 Controles contra códigos móveis

10. Gerenciamento das Operações e Comunicações

- 10.5 Cópias de segurança
- 10.5.1 Cópias de segurança das informações
-
- 10.6. Gerenciamento da segurança em redes
- 10.6.1 Controles de redes
- 10.6.2 Segurança dos serviços de rede

10. Gerenciamento das Operações e Comunicações

- 10.7. Manuseio de mídias
- 10.7.1 Gerenciamento de mídias removíveis
- 10.7.2 Descarte de mídias
- 10.7.3 Procedimentos para tratamento de informação
- 10.7.4 Segurança da documentação dos sistemas

10. Gerenciamento das Operações e Comunicações

- 10.8. Troca de informações
- 10.8.1 Políticas e procedimentos para troca de informações
- 10.8.2. Acordos para a troca de informações
- 10.8.3 Mídias em trânsito
- 10.8.4 Mensagens eletrônicas
- 10.8.5 Sistemas de informações do negócio

10. Gerenciamento das Operações e Comunicações

- 10.9 Serviços de comércio eletrônico
- 10.9.1 Comércio eletrônico
- 10.9.2 Transações on-line
- 10.9.3 Informações publicamente disponíveis

10. Gerenciamento das Operações e Comunicações

- 10.10 Monitoramento
- 10.10.1 Registro de auditoria
- 10.10.2 Monitoramento do uso do sistema
- 10.10.3 Proteção das informações dos registros (logs)
- 10.10.4 Registros (logs) de administrador e operador
- 10.10.5 Registros (logs) de falhas
- 10.10.6 Sincronização de relógios

11. Controle de Acessos

- 11.1. Requisitos de Negócio para Controle de Acesso
 - 11.1.1 Política de controle de acesso
- 11.2. Gerenciamento de acesso do usuário
 - 11.2.1 Registro de usuário
 - 11.2.2 Gerenciamento de privilégios
 - 11.2.3 Gerenciamento de senha do usuário
 - 11.2.4 Análise crítica dos direitos de acesso de usuário

11. Controle de Acessos

- 11.3 Responsabilidades dos Usuários
 - 11.3.1 Uso de senhas
 - 11.3.2 Equipamentos de usuários sem monitoração
 - 11.3.3 Política de mesa limpa e tela limpa

11. Controle de Acessos

- 11.4. Controle de acesso à rede
 - 11.4.1 Política de uso dos serviços de rede
 - 11.4.2 Autenticação para conexão externa do usuário
 - 11.4.3 Identificação de equipamento em redes
 - 11.4.4 Proteção e configuração de portas de diagnóstico remotas
 - 11.4.5 Segregação de redes
 - 11.4.6 Controle de conexão de rede
 - 11.4.7 Controle de roteamento de redes

11. Controle de Acessos

- 11.5 Controle de acesso ao sistemas operacional
- 11.5.1 Procedimentos seguros de entrada no sistema (logon)
- 11.5.2 Identificação e autenticação de usuário
- 11.5.3 Sistemas de gerenciamento de senha
- 11.5.4 Uso de utilitários de sistema
- 11.5.5 Desconexão de terminal por inatividade
- 11.5.6 Limitação de horário de conexão

11. Controle de Acessos

- 11.6. Controle de acesso à aplicação e à informação
 - 11.6.1 Restrição de acesso à informação
 - 11.6.2 Isolamento de sistemas sensíveis
 -
- 11.7. Computação móvel e trabalho remoto
 - 11.7.1 Computação e comunicação móvel
 - 11.7.2 Trabalho remoto

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- 12.1. Requisitos de segurança de sistemas de informação
- 12.1.1 Análise e especificação dos requisitos de segurança

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- 12.2. Processamento correto nas aplicações
- 12.2.1 Validação dos dados de entrada
- 12.2.2 Controle do processamento interno
- 12.2.3 Integridade de mensagens
- 12.2.4 Validação de dados de saída

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- 12.3. Controles Criptográficos
 - 12.3.1 Política de uso de controles criptográficos
 - 12.3.2 Gerenciamento de chaves
 -
- 12.4. Segurança dos arquivos do sistema
 - 12.4.1 Controle de software operacional
 - 12.4.2 Proteção dos dados para teste de sistema
 - 12.4.3 Controle de acesso ao código-fonte de programa

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- 12.5. Segurança em processos de desenvolvimento e de suporte
 - 12.5.1 Procedimentos para controle de mudanças
 - 12.5.2 Análise crítica técnica das aplicações após mudanças no sistema operacional
 - 12.5.3 Restrições sobre mudanças em pacotes de software
 - 12.5.4 Vazamento de informações
 - 12.5.5 Desenvolvimento terceirizado de software

12. Aquisição, desenvolvimento e manutenção de sistemas de informação

- 12.6. Gestão de vulnerabilidades técnicas
- 12.6.1 Controle de vulnerabilidades técnicas

13. Gestão de Incidentes de Segurança da Informação

- 13.1. Notificação de fragilidades e eventos de segurança da informação
 - 13.1.1 Notificação de eventos de segurança da informação
 - 13.1.2 Notificação de fragilidades de segurança da informação
 -

13. Gestão de Incidentes de Segurança da Informação

- 13.2. Gestão de incidentes de segurança da informação e melhorias
 - 13.2.1 Responsabilidades e procedimentos
 - 13.2.2 Aprendendo com os incidentes de segurança da informação
 - 13.2.3 Coleta de evidências

14. Gestão da continuidade do negócio

- 14.1 Aspectos da gestão da continuidade, relativos à segurança da informação
 - 14.1.1 Incluindo segurança da informação no processo de gestão da continuidade de negócio
 - 14.1.2 Continuidade de negócios e análise/avaliação de riscos
 - 14.1.3 Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
 - 14.1.4 Estrutura do plano de continuidade do negócio
 - 14.1.5 Testes, manutenção e reavaliação dos planos de continuidade do negócio

15. Conformidade

- 15.1. Conformidade com requisitos legais
 - 15.1.1 Identificação da legislação vigente
 - 15.1.2 Direitos de propriedade intelectual
 - 15.1.3 Proteção de registros organizacionais
 - 15.1.4 Proteção de dados e privacidade de informações pessoais
 - 15.1.5 Prevenção de mau uso de recursos de processamento da informação
 - 15.1.6 Regulamentação de controles de criptografia

15. Conformidade

- 15.2. Conformidade com normas e políticas de segurança da informação e conformidade técnica
- 15.2.1 Conformidade com as políticas e normas de segurança da informação
- 15.2.2 Verificação da conformidade técnica

15. Conformidade

- 15.3 Considerações quanto à auditoria de sistemas de informação
- 15.3.1 Controles de auditoria de sistemas de informação
- 15.3.2 Proteção de ferramentas de auditoria de sistemas de informação

Plano de Continuidade do Negocio

BCP - Business Continuity Plan

BCP

- É o desenvolvimento de planos de ação e estratégias para garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.
- O funcionamento de uma empresa deve-se a duas variáveis :
 - Componentes;
 - Processos;

- Plano de continuidade do Negocio se divide em:
 - Plano de Administração de Crises
 - Plano de Recuperação de Desastres
 - Plano de Continuidade Operacional



Marcos Monteiro

<http://www.marcosmonteiro.com.br>