Ciência da Computação Integrada - CCI

Aulas 3, 4, 5, 6 e 7

2º Semestre de 2017

Prof. Vaine Luiz Barreira

http://bit.ly/Unip17

Segurança da Informação - SI

A segurança da informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

"A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida."

Norma NBR ISO/IEC 27002

Glossários de SI

Os glossários são ótimas referências quando precisamos validar alguma definição ou um conceito, mas também podem ser úteis como forma de aprendizagem.

Glossário da Cartilha de Segurança para Internet do Cert.br
http://cartilha.cert.br/glossario

Glossário de Segurança da Microsoft
http://www.microsoft.com/brasil/security/glossary.mspx

Glossário de segurança na Internet da Symantec
https://www.symantec.com/pt/br/theme.jsp?themeid=glossario-de-seguranca

Quanto vale a informação?

Qual é o valor das informações? Com base nas respostas de 500 profissionais de TI na América Latina, a estimativa é que 50 por cento do valor de mercado das organizações deriva das informações que elas possuem.

Os entrevistados afirmam que

informações = 50%

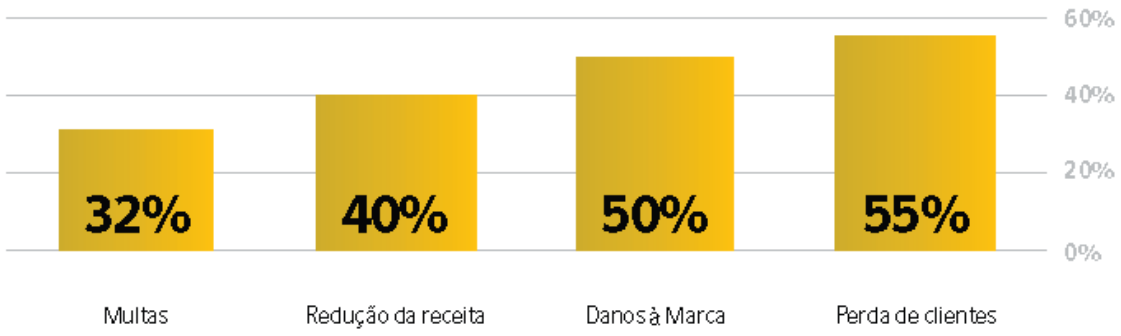
do valor de mercado das organizações

Quanto custa a perda?

As consequências de perder algumas ou todas as informações seriam devastadoras para os negócios. Quando se perguntou aos entrevistados o que aconteceria se as informações de sua organização se perdessem irremediavelmente sem chance de recuperação, as respostas incluíram: perda de clientes (55 por cento), danos à marca (50 por cento), redução na receita (40 por cento) e multas (32 por cento).

A perda dessas informações seria **catastrófica**

Consequências da perda de informações de negócios



O mercado do Cibercrime

Mais que a soma do que movimentam o tráfico de drogas e o tráfico de armas

Fonte: Cybersecurity Ventures - Cybersecurity Economic Predictions

Symantec Cibercrime Report 2013

- 60% dos brasileiros foram vítimas do cibercrime.
- 45% dos adultos no país tiveram uma experiência de crime virtual e comportamento de risco nos últimos 12 meses.
- Custo líquido do crime cibernético, nos últimos 12 meses, foi superior a R$ 18 bilhões.
- 57% dos usuários de smartphone no Brasil foram vítimas de crime virtual móvel.
- 39% dos usuários de smartphone no Brasil afirmam que não deletam e-mails suspeitos de pessoas que não conhecem. (CSRF)
- 33% dos brasileiros não se desconecta dos perfis sociais após o acesso e 31% se conecta com pessoas desconhecidas. (Session Hijacking / Fixation)
- 61% dos adultos brasileiros disseram utilizar redes de Wi-Fi públicas ou inseguras.

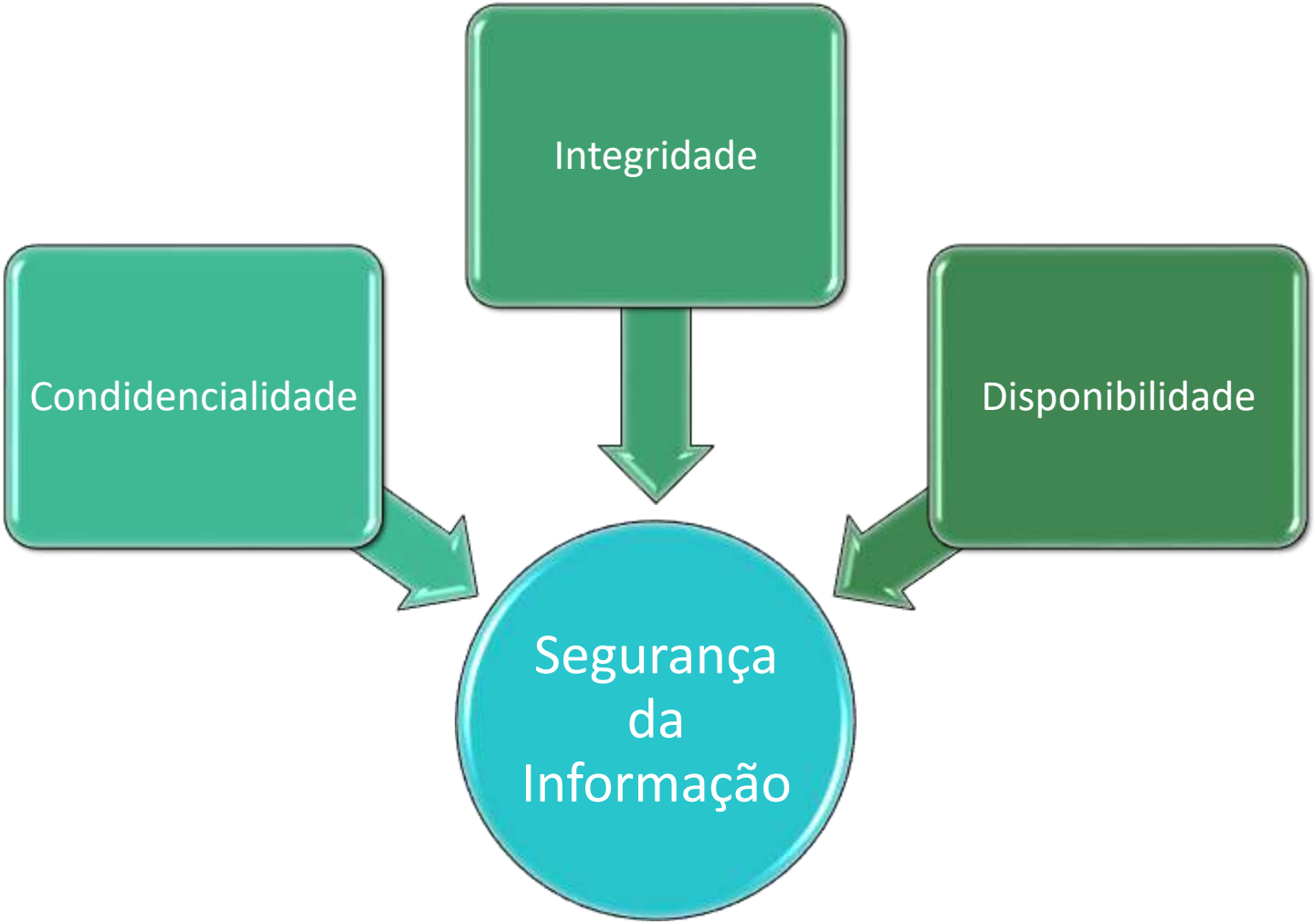
Características da SI

São características básicas da segurança da informação os atributos de CID:

- ✓ Confidencialidade
- ✓ Integridade
- ✓ Disponibilidade

Não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

Características da SI



Pilares da SI

- ✓ Confidencialidade

  garantir que a informação seja acessível somente por quem possui autorização do proprietário da informação para acessar

- ✓ Integridade

  garantir a salvaguarda da exatidão e completeza da informação e dos métodos de processamento

- ✓ Disponibilidade

  garantir que a informação esteja sempre acessível e disponível quando necessário, por aqueles usuários autorizados

Pilares da SI

Outros atributos importantes são a irretratabilidade, a autenticidade e a conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

- ✓ Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

- ✓ Irretratabilidade - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

- ✓ Conformidade - propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

Cenário Mundial Atual

- Grandes corporações e governos sofrendo invasões
- Uso massivo de redes sociais
- Ataques direcionados em vários países
- Malwares focados em mobile

Cenário Mundial Atual

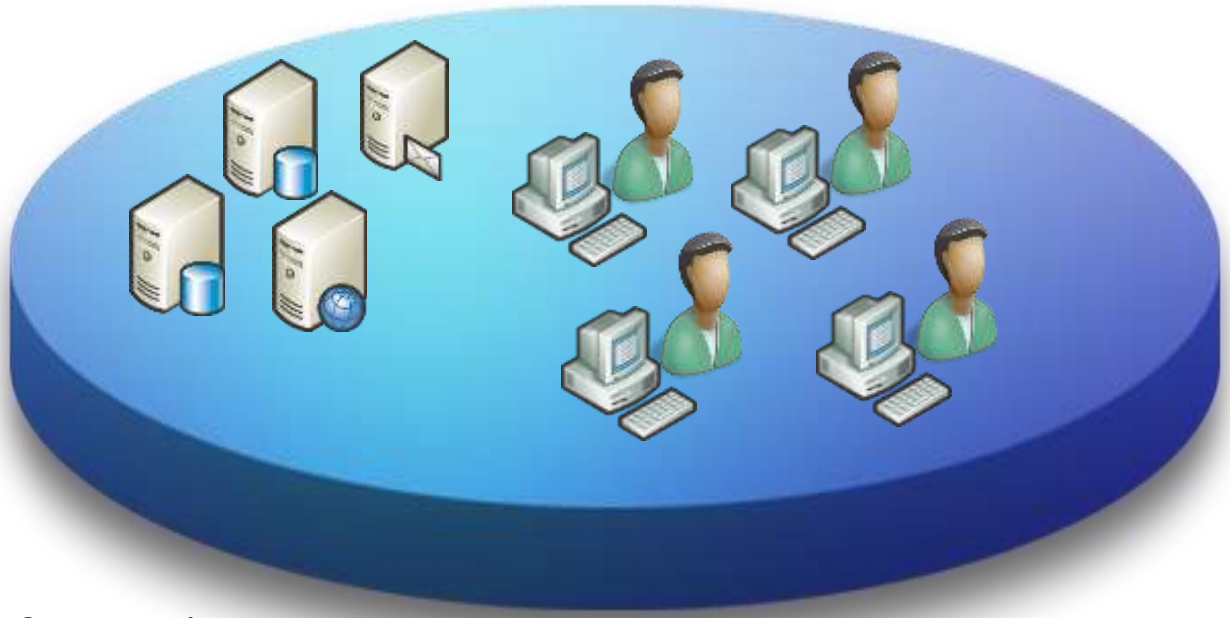
TARGET

Segundo a Forbes, os impactos financeiros que esse roubo de dados causou:

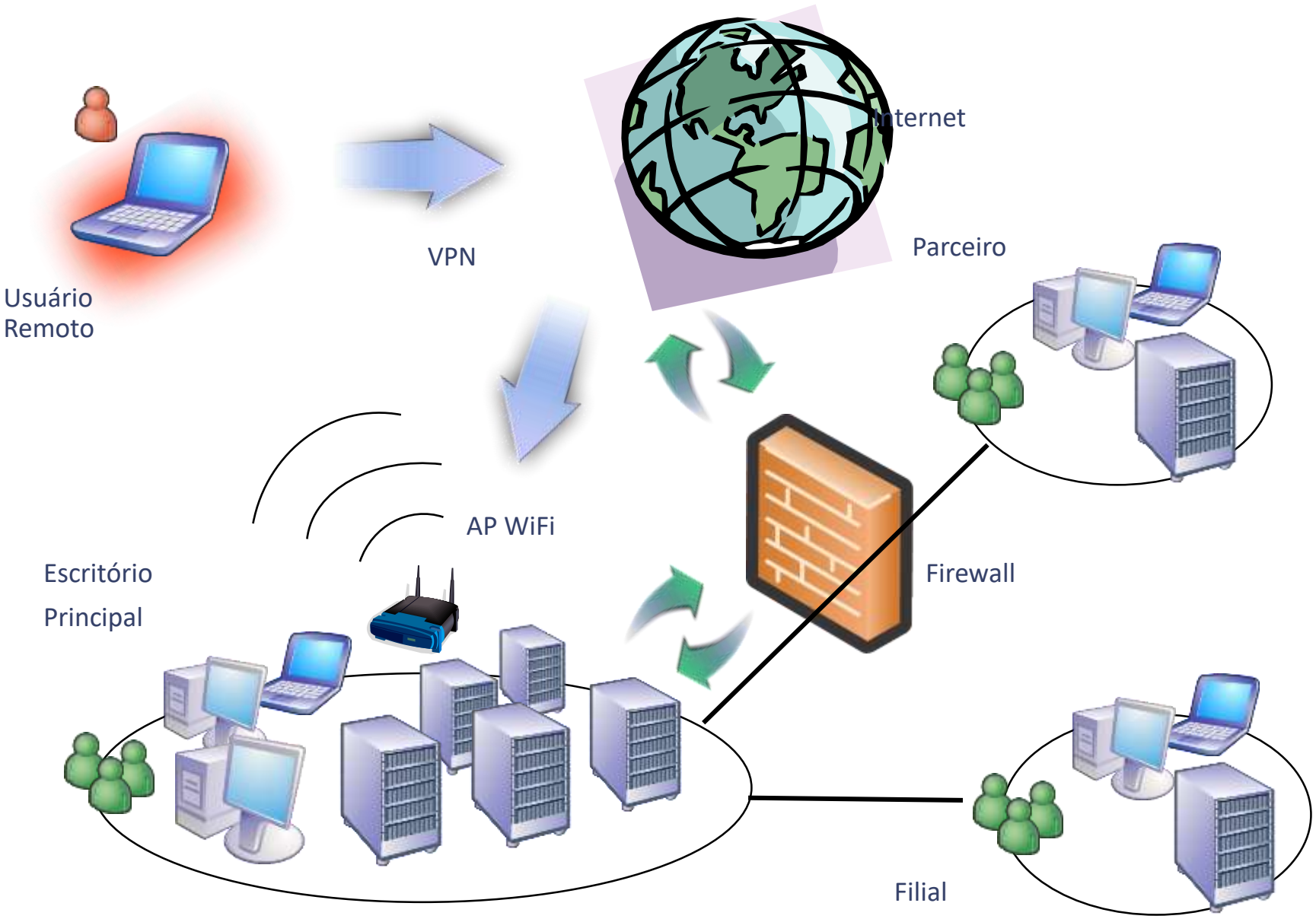
- Seu lucro no quarto trimestre de 2013 caiu quase 50%;
- O lucro anual da Target em 2013, no total de US$ 1.97 bilhões, caiu mais de um terço (34.3%);
- As ações caíram 9% desde o anúncio do roubo de dados;
- A Target gastou US$ 17 milhões com o roubo de dados em 2013, e não sabe qual será o custo total que ela terá que arcar durante 2014 por causa do incidente.

Os maiores incidentes de 2016

Antes o perímetro era claro

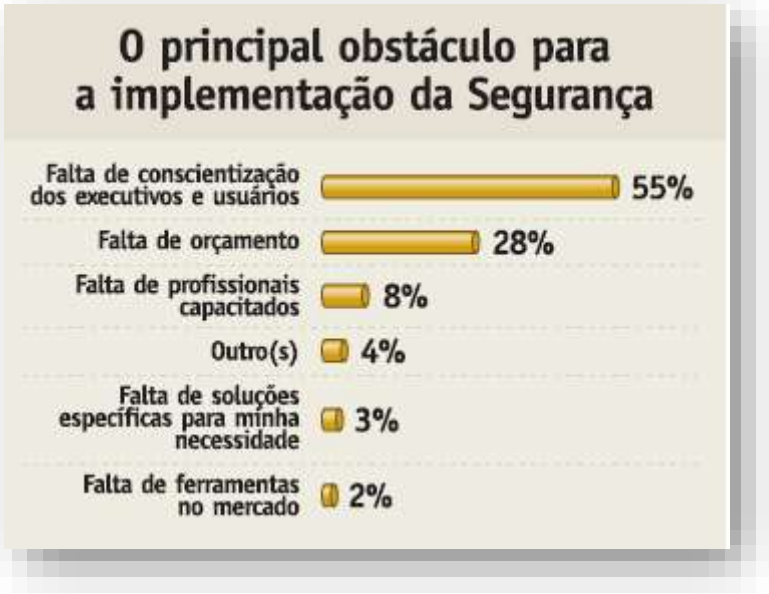


Rede Corporativa


Internet
VPN
Usuário
Remoto
Parceiro
AP WiFi
Escritório
Principal
Firewall
Filial

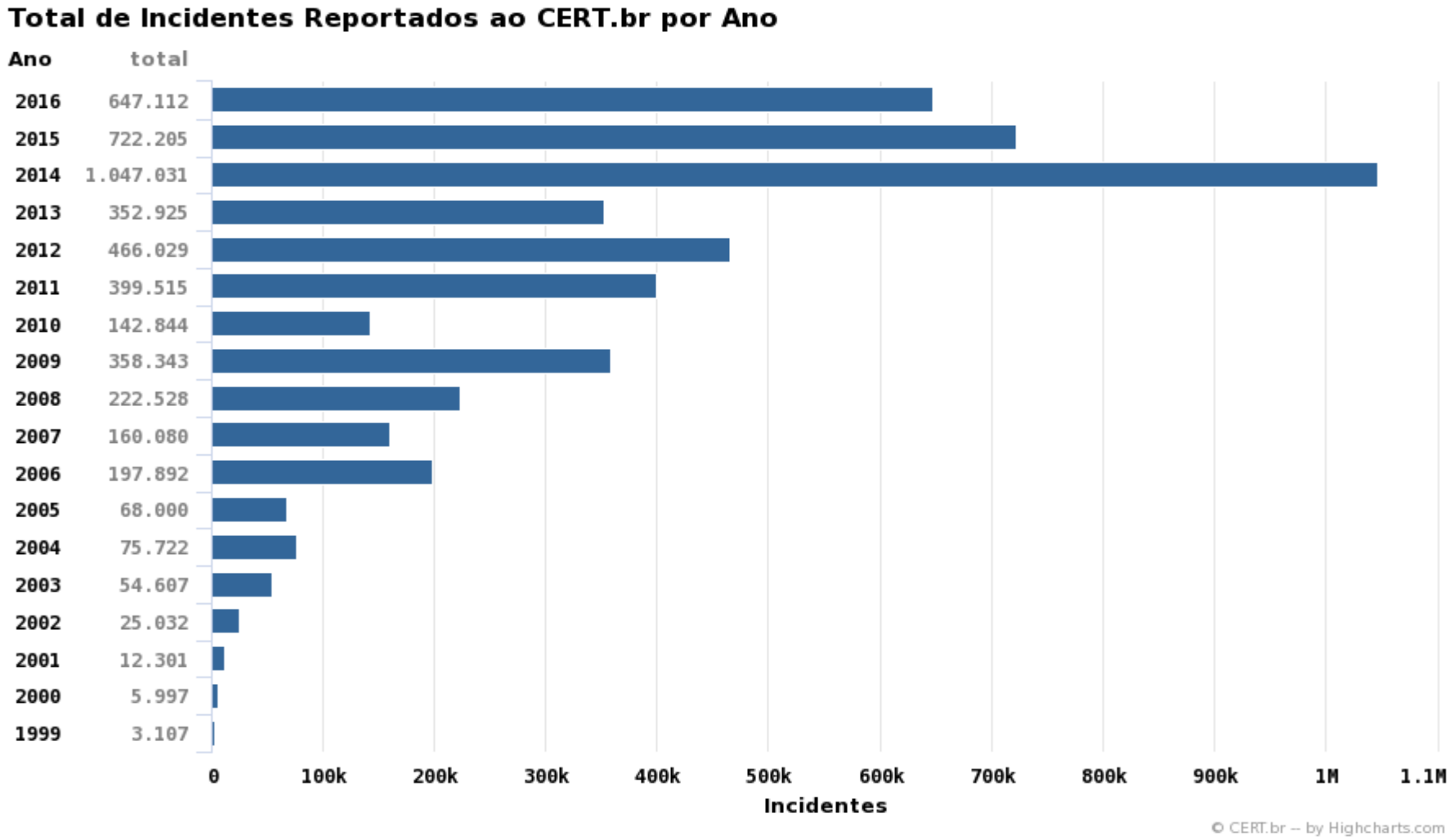
Segurança da Informação

- A maior dificuldade em implementar segurança não é tecnológica, e sim organizacional
- Conhecimento é a chave da segurança
  segurança carece de base teórica
- Segurança tem que ser cíclica
  sempre revendo os processos
- Profissional pró-ativo e não reativo



Total de Incidentes

Valores acumulados: 1999 a 2016 novo



Ondas da SI

1- Segurança voltada ao Mainframe
   fornecedor provia segurança

2- Segurança das redes heterogêneas
   protocolos e SOs heterogêneos

3- Segurança na Internet
   foco em IP

4- Legislação e regulamentação
   Sarbanes-Oxley 2002

5- Segurança da Computação em Nuvem

6- Segurança de Internet das Coisas (IoT)

Legislação e Regulamentação

- ITIL 3, Cobit 5, MOF 4

  governança, risco e compliance de TI

- ISO 20.000

  gestão de serviços de TI

- Série ISO 27.000

  gestão de segurança da informação

Governança de TI

As empresas estão sacrificando dinheiro, produtividade e vantagem competitiva por não implementar uma Governança de TI eficaz.

Os executivos precisam de uma maneira melhor de:

- Dirigir a TI para obtenção de benefícios.
- Medir o Valor fornecido pela TI.
- Gerenciar os Riscos pertinentes a área de TI.

Governança Segurança da Informação

Governança da Segurança da Informação é o conjunto de processos, controles e demais atividades com o propósito de garantir que:

- a gestão do programa corporativo de segurança da informação está orientada aos objetivos de negócio;
- exista uma avaliação contínua das políticas, padrões, procedimentos e riscos em segurança da informação; e
- os riscos em segurança da informação estejam em níveis aceitáveis pela organização.

Uma boa governança garante que as prioridades e os investimentos em segurança da informação estão de acordo com as prioridades e objetivos da organização.

Gestão de Segurança da Informação

A gestão cuida da execução eficiente e eficaz das atividades previstas para o processo de segurança. Ela tem como objetivo garantir a existência de controles para a proteção da informação, em todas as dimensões existentes, necessária para a realização do negócio e alcance dos objetivos do negócio da Organização.

A Gestão é o como fazer acontecer a segurança da informação.

Sustentabilidade de Segurança da Informação

- Sustentabilidade do processo de segurança da informação é o conjunto de ações e decisões que devem existir para que este processo:
- seja continuo ao longo do tempo,
- permita que este processo se retro alimente,
- permita que a organização aprenda,
- possibilite que as perdas e impactos que o processo de segurança impediu que a organização sofresse, tornem-se os geradores de recursos para o patrocínio deste processo.

Sem dúvida alguma o apoio da alta direção da Organização e o alinhamento aos objetivos de negócio são críticos para que haja esta sustentabilidade.

Governança, Gestão e Sustentabilidade

Governança
O que se quer: Priorização

Gestão
Como fazer acontecer o que se quer

Sustentabilidade
Como garantir que, o que se quer, será alcançado sempre ao longo do tempo

ITIL

Conjunto de Melhores Práticas que orientam o Gerenciamento de Serviços de TI.

Consiste em uma série de publicações que fornecem recomendações para o provisionamento da Qualidade dos Serviços de TI e dos Processos e recursos necessários para suportá-los.

Trata de “como” fazer os Serviços de TI.

5 Volumes:
1-Estratégia de Serviço
2-Desenho de Serviço
3-Transição de Serviço
4-Operação de Serviço
5-Melhoria Contínua de Serviço

26 Processos, como:
Gerenciamento de Capacidade, Disponibilidade, Mudança, Seg.Info

ITIL – para que usar?

Como foca na medição contínua e na melhoria da qualidade dos serviços entregues pela área de TI, de uma perspectiva do negócio e do cliente, proporciona uma série de benefícios às empresas, incluindo:

- Aumento da satisfação dos clientes em relação aos serviços prestados pela TI.
- Aumento da disponibilidade dos serviços, levando diretamente a aumento dos lucros e resultados.
- Economia advinda da redução de trabalho, tempo perdido, melhoria do gerenciamento e uso de recursos.
- Melhoria do tempo de disponibilização de novos produtos e serviços.
- Melhoria da tomada de decisão e otimização de riscos.

CoBIT

Conjunto de Ferramentas que garante que a área de TI está trabalhando efetivamente.

Funciona como um framework abrangente.

Fornece linguagem comum para se comunicar metas, objetivos e resultados esperados para todos os interessados.

Baseado em boas práticas em:

- Alinhamento estratégico da TI com os objetos de negócio
- Valor dos serviços prestados e novos projetos
- Gerenciamento de risco
- Gerenciamento de recursos
- Gerenciamento de desempenho (performance)

Trata “do que” fazer nos Serviços de TI.

CoBIT

Princípios do Cobit 5:

1. Satisfazer as necessidades das partes interessadas;
2. Envolver todas as áreas da empresa;
3. Empregar uma estrutura única e integrada;
4. Possibilitar uma abordagem holística;
5. Separar governança de gerenciamento.

ISO 20.000

A ISO 20.000 é um conjunto que define as melhores práticas de gerenciamento de serviços de TI, e tem a intenção de ser completamente compatível com o ITIL.
São requisitos da norma definição de políticas, objetivos, procedimentos e processos de gerenciamento para assegurar a qualidade efetiva na prestação de serviços de TI.

Os processos da ISO/IEC 20 000 são os seguintes:

- processos de planejamento e implementação (PDCA);
- processos de entrega de serviços;
- processos de relacionamento;
- processos de solução, liberação e controle.

Série ISO 27.000

As normas da família ISO 27000 convergem para um ponto, o Sistema de Gestão de Segurança da Informação (SGSI), tendo como as normas mais conhecidas as ISO 27.001 e ISO 27.002.

Estão muito relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos.

O SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade.

Série ISO 27.000

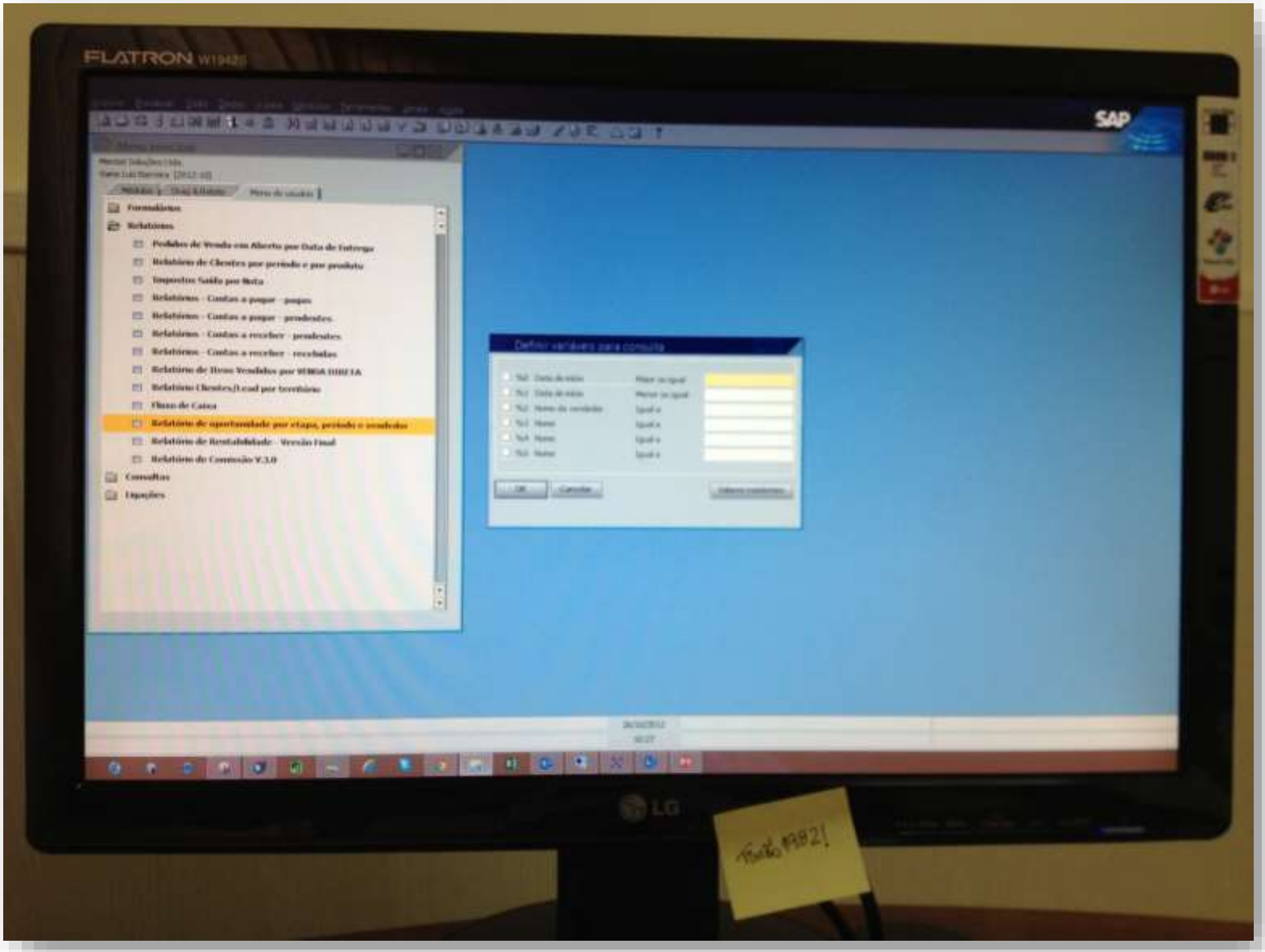
A família ISO 27.000 é grande, alguns exemplos:

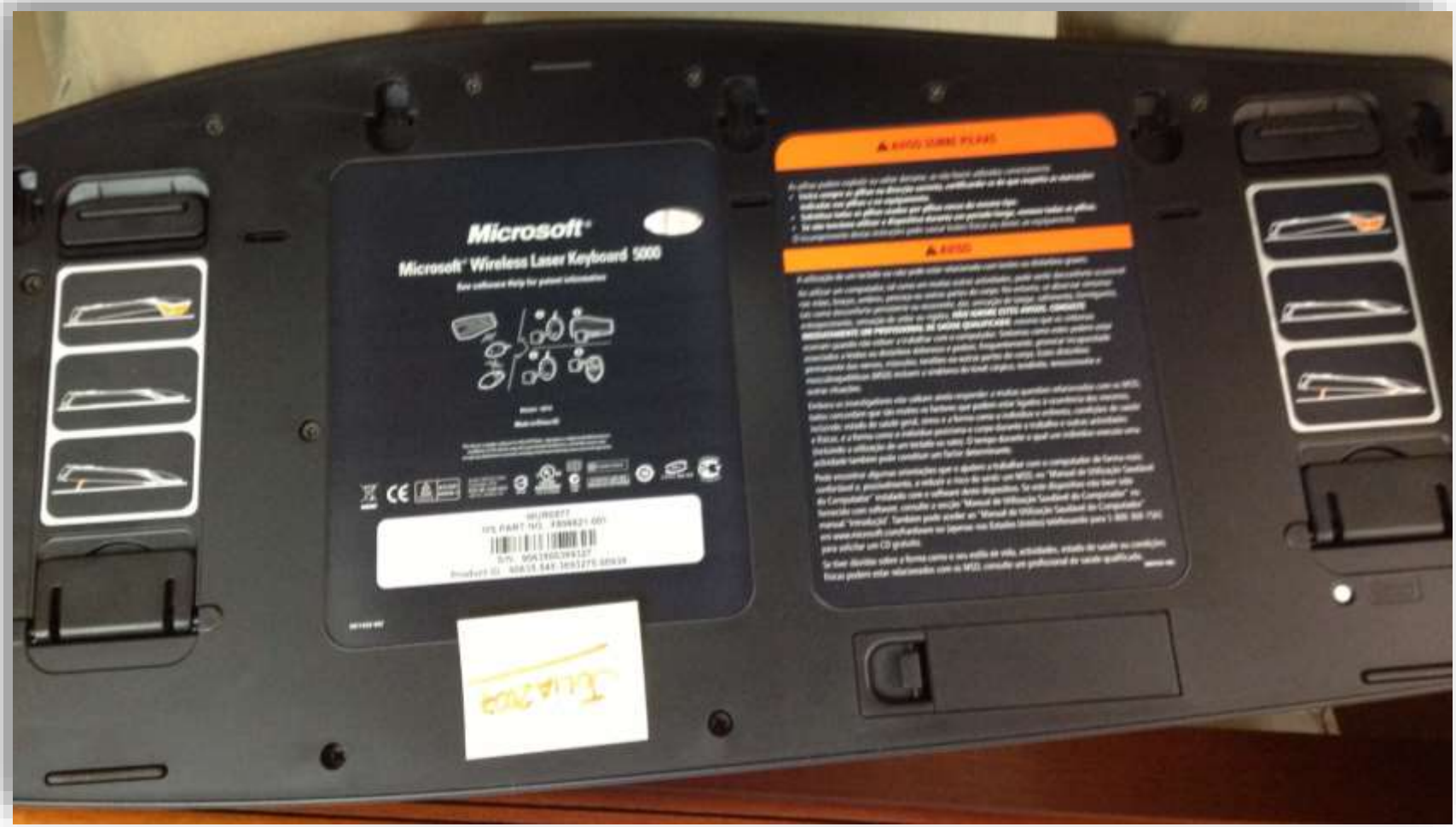
- ISO 27.000 – Traz informações básicas sobre as normas da série.
- ISO 27.001 – Bases para a implementação de um SGSI em uma organização.
- ISO 27.002 – Certificação profissional, traz códigos de práticas para profissionais (apresenta 133 controles para a Política de Segurança da Informação).
- ISO 27.003 – Diretrizes mais específicas para implementação do SGSI.
- ISO 27.004 – Normas sobre as métricas e relatórios do SGSI.
- ISO 27.005 – Norma sobre gestão de riscos do SGSI.
- ISO 27.017 – Controles Computação em Nuvem
- ISO 27.033 – Segurança de Redes (6 partes)
- ISO 27.037: orientações para a identificação, coleta, aquisição e preservação de evidências forenses digitais.

Segurança da Informação

Problema é a falsa sensação de segurança.


You've taken precautions. Your data's protected.
Absolutely. You sure?


FLATRON
SAP
Definir variáveis para consulta
LG


Microsoft
Microsoft Wireless Laser Keyboard 5000


ESPN
BASEBALL TONIGHT
UPDATE
FANTASY IMPACT
FREEMAN (ATL) 1-4, HR(4) 2 RBI
KEMP: 1-4 HR (12) RBI
DODGERS 2 ROCKIES 6
MIL vs SD UPDATE
DELMON YOUNG SUSPENDED
SSID: MLB-Press
Password: BWAA#2012
SSID: MLB-Photo
Password: Photo#2012
MLB
me last week after fight outside New York hotel during which police sa


internal requests:
ccpi.cgci@dpf.gov.
Brasil
2014
wifi network: WORLDCUP
Password: 65a2112014


Wi-Fi Access
marko
w3LcOm3!!!ERE
PASSWORD
case-sensitive
"Forget" or "Remove"
CBS
THIS
MORNING
SUPER BOWL SECURITY
INSIDE SECRET, FIRST-OF-ITS-KIND

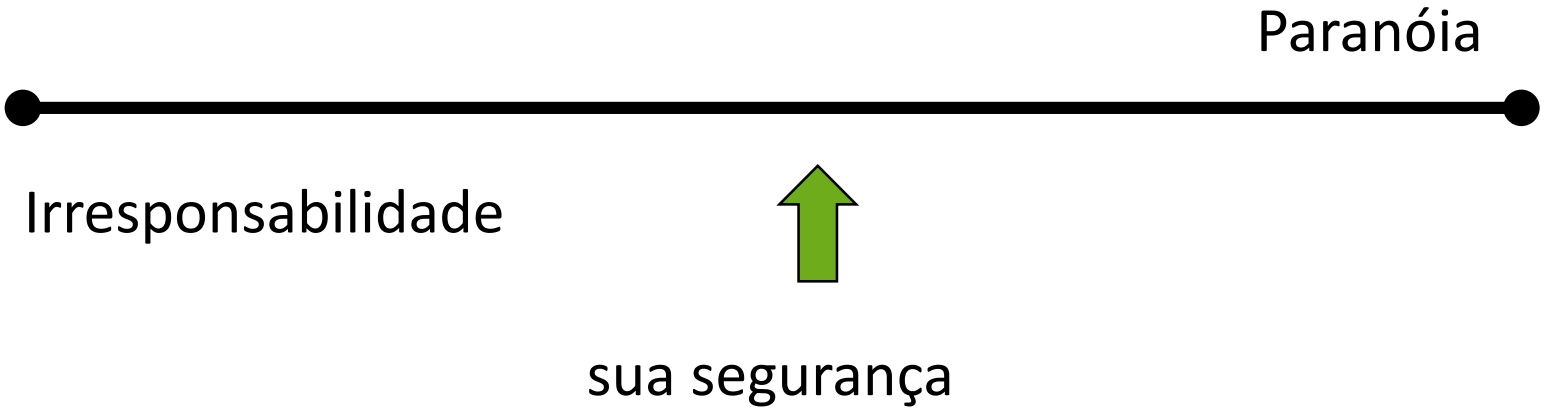

EWS HD
Emergency Out of hrs
Username:- EmergencyPlanning
Password:- Winter14
USE ONLY THE DRY WIPE PENS PROVIDED
ME WEATHER
Flood
PLANNER SIMON PARKER
3 mins
ARGES VARY) OR TWEET @SkyNews
NEWS ALERT
EXTREME WEATHER: FULL WEATHER AND TRAV


data
Person
Vehicle
Phone
Places
CNN

Elétrica fácil

Vídeo

Calibrar a Segurança

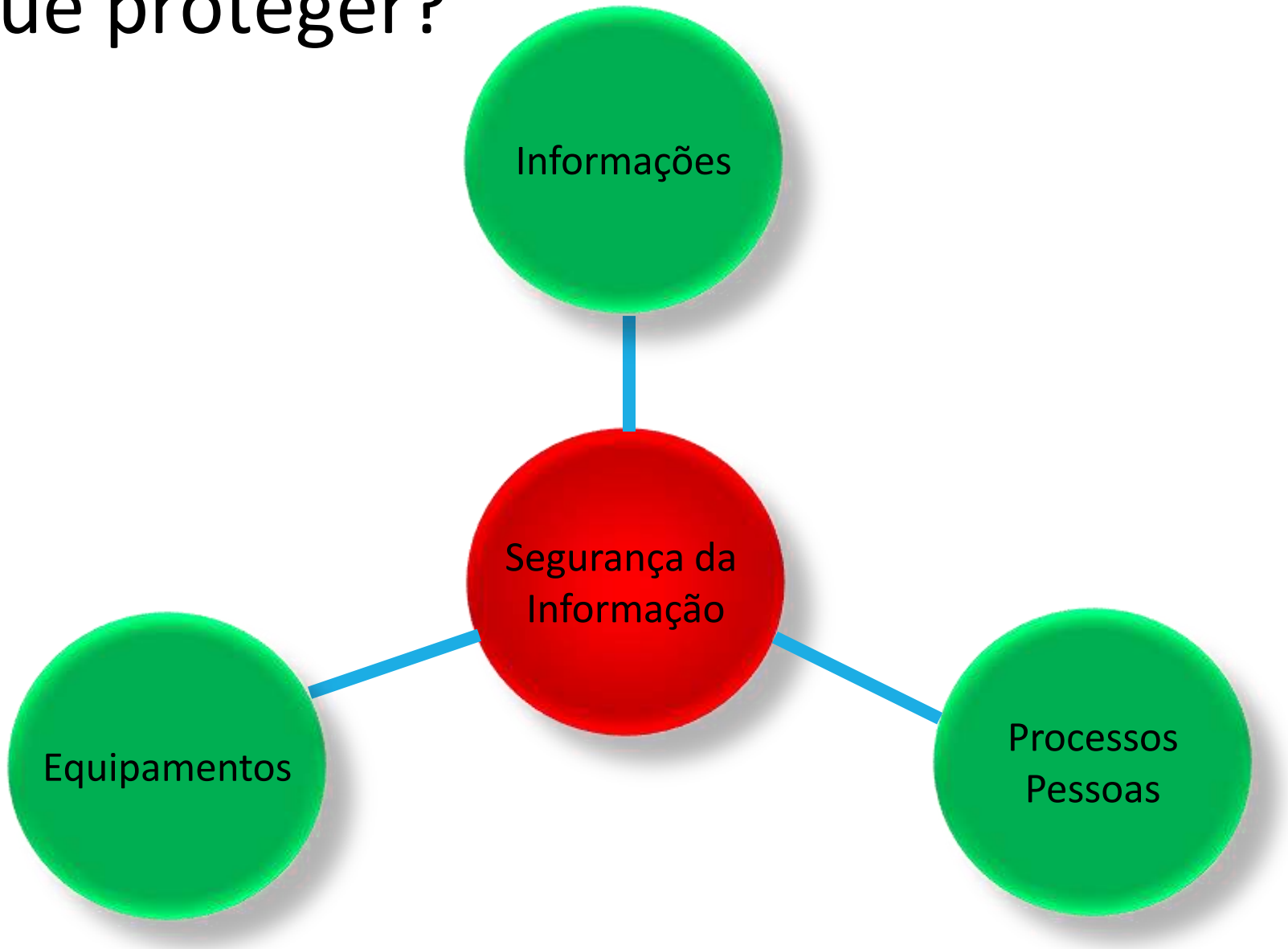


Qual o mercado da empresa ?

Qual a estratégia ?

Qual o orçamento ?

O que proteger?



Agentes da SI

- ✓ Gestor da Informação

  Gestor ou área responsável pela informação. Cabe ao gestor classificar a informação e deliberar sobre as proteções que deverão ser aplicadas aos seus ativos de informação.

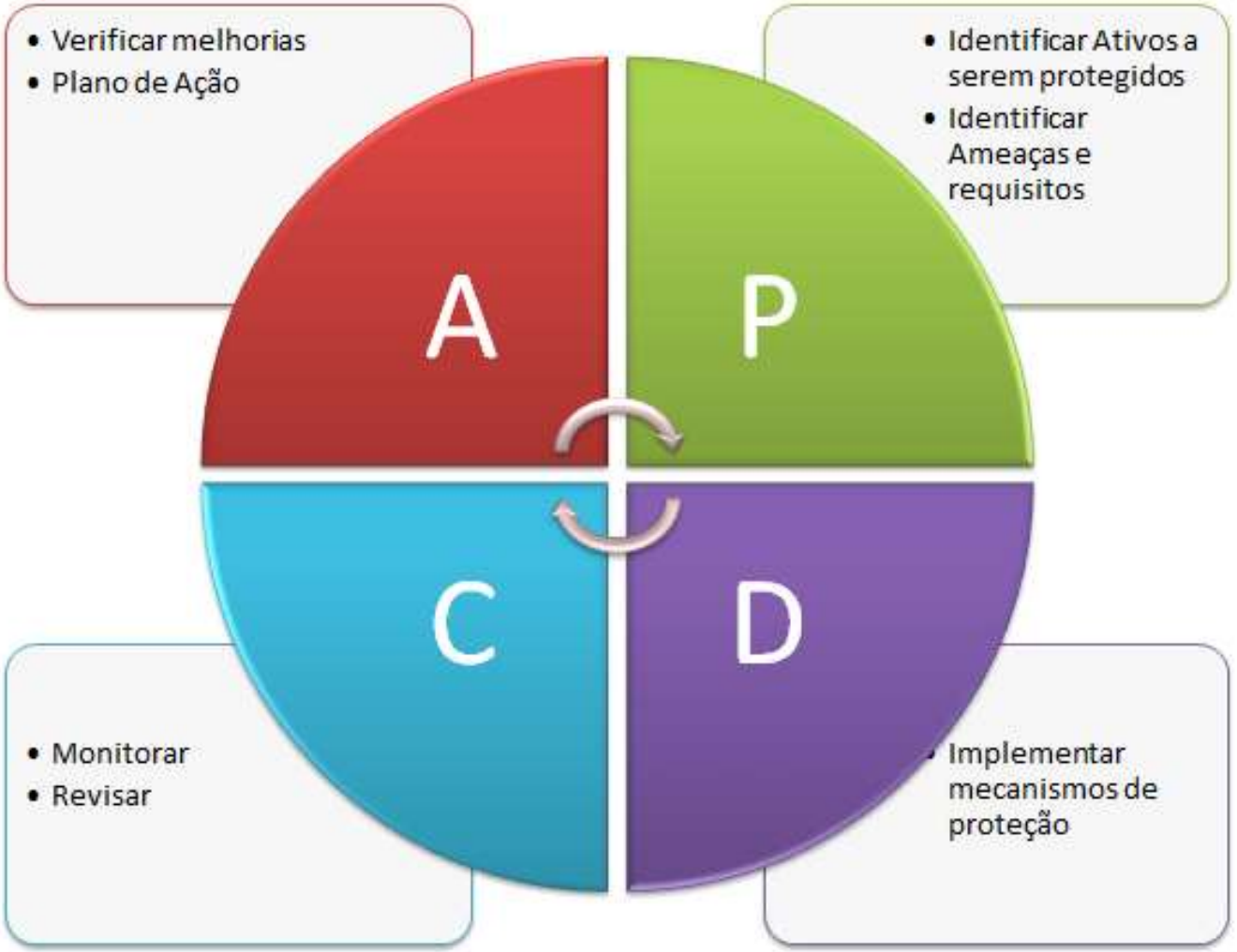
- ✓ Custodiante

  Pessoa ou área dentro da organização responsável pelo processamento, organização e guarda da informação. Normalmente a área de TI.

- ✓ Usuário

  Pessoa que interage diretamente com a informação em suas diversas formas. Cabe ao usuário zelar pelas informações que manipula.

Ciclo de Segurança



Ciclo de Segurança

A implementação de uma política de segurança da informação segue o modelo do ciclo **PDCA (ou ciclo de Deming),** onde temos quatro passos:

- **Planejar (Plan):** Neste passo devemos identificar os ativos a serem protegidos através da análise de riscos;
- **Realizar (Do):** Uma vez definido os ativos a serem protegidos, bem como as ameaças, devemos colocar em ação o planejamento realizado e aplicar os mecanismos necessários para atender os requisitos de proteção identificados;
- **Verificar (Check):** Após a implementação do plano através do passo anterior, devemos monitorar se o plano está sendo seguido e se necessita ser revisado;
- **Agir (Act):** Após a monitoração e revisão, é necessário ter um plano de ação para reiniciar o ciclo e planejar mudanças na política estabelecida no plano anterior.

Ameaças à SI

Ameaça é todo e qualquer perigo eminente, seja natural, humano, tecnológico, físico ou político-econômico.

Tipos de ameaças:

- Vandalismo
- Roubo ou furto
- Sabotagem
- Incêndio
- Inundação
- Falha de servidores
- Falha humana
- Acesso de pessoas não autorizadas

Ameaças à SI

Malwares

Termo genérico que se refere a todos os tipos de programas que executam ações maliciosas em um computador.

Exemplos de malware:

- Vírus
- Verme (worm)
- Cavalo de Tróia (trojan horse)
- Software espião (spyware)

Vírus

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo (infectando) nos sistemas afetados, ou tornando-se parte de outros programas e arquivos de um computador.
O vírus depende de uma ação do usuário para que possa se tornar ativo e dar continuidade ao processo de infecção.

Worms

Worm é um programa capaz de se propagar automaticamente através das redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não necessita ser explicitamente executado na máquina da vítima para se propagar. Sua propagação se dá através da exploração de vulnerabilidades (exploits) existentes ou falhas na configuração de softwares instalados em computadores.

Trojan Horses

É um programa normalmente recebido como um “presente” (por exemplo cartão virtual, álbum de fotos, protetor de tela, jogo, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Spywares

Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar informações coletadas para terceiros.

Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

SPAM e Phishing

Dá-se o nome de SPAM a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Phishing é uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros, ao acesso de páginas fraudulentas na Internet ou a instalação de códigos maliciosos.

Medidas de Segurança

As medidas de segurança para proteger a informação podem ser:

- Físicas
- Tecnológicas
- Organizacionais

Físicas

- Perímetro de segurança (paredes, portas, portões, etc)
- Autenticação (também para controle lógico)
  - o que você sabe?
  - o que você tem?
  - o que você é?
- Biometria
- Política de mesa limpa
- No-break
- Climatização
- Interferência eletromagnética

Tecnológicas

- Gerenciamento de acesso lógico
  - Tríade conhecida como “Triplo A”:
  - Autenticação – identificação da identidade
  - Autorização – liberação de acesso
  - Auditoria – registro das solicitações de acesso
- Firewall
- Cópias de segurança (backup)
- Criptografia
- Certificado digital
- Rede Privada Virtual (VPN)

Organizacionais

- Classificação da informação
- Gestão de mudanças
- Segregação de funções e gestão de acesso
- Gerenciamento da continuidade dos negócios
- Plano de recuperação de desastres

Engenharia Social

A seguir serão apresentadas 6 técnicas mais utilizadas pelos Engenheiros Sociais:

- Analise do Lixo
- Internet e Redes Sociais
- Contato Telefônico
- Abordagem Pessoal
- Phishing
- Falhas Humanas

As senhas mais comuns de 2016

1. 1- 123456
2-123456789
3- qwerty
4- 12345678
5- 111111
6- 1234567890
7- 1234567
8- password
9- 123123
10- 987654321
11- qwertyuiop
12- mynoob
13- 123321
14- 666666
15- 18atcskd2w
16- 7777777
17- 1q2w3e4r
18- 654321
19- 555555
20- 3rjs1la7qe
21- google
22- 1q2w3e4r5t
23- 123qwe
24- zxcvbnm
25- 1q2w3e

Desafios da SI

- Acesso seguro de qualquer lugar
- Expansão do perímetro de segurança
- Variedade de dispositivos móveis e IoT
- Educação dos usuários
- Virtualização de recursos
- Dados armazenados na nuvem





Smartphones e Tablets

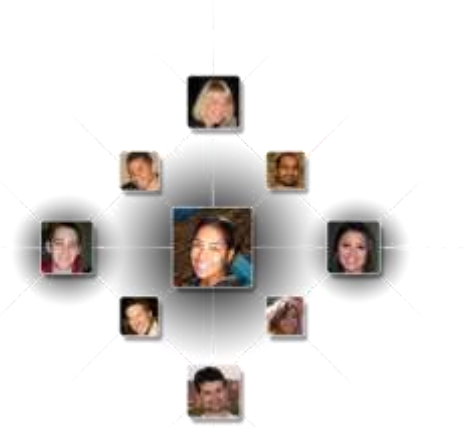
- Novos recursos, novos riscos
- Como controlar?
- Sempre conectados
- Câmeras e armazenamento

Segurança de dispositivos móveis

- Não abra tudo que receber (e-mails, SMS, links)
- Tenha uma senha “forte” no dispositivo
- Mantenha-o atualizado
- Desative o que não usa (principalmente bluetooth e gps)
- Administração pela equipe de TI (independente do SO)
- Remote Wipe

Redes Sociais

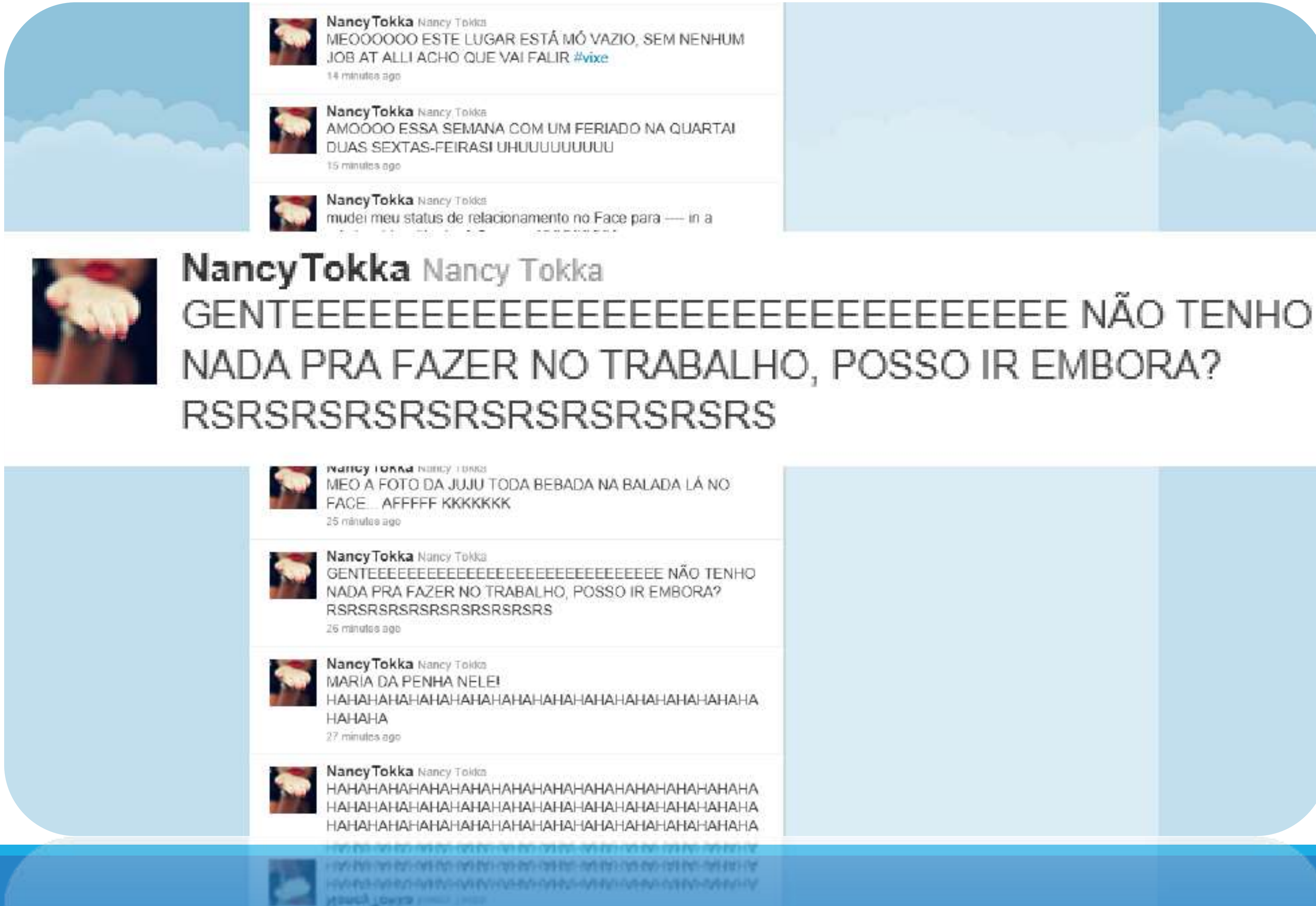
- Realidade nas corporações
- Uso massivo e crescente
- Novo cenário de privacidade



facebook twitter LinkedIn flickr

YouTube foursquare skype

Cuidado com o que escreve

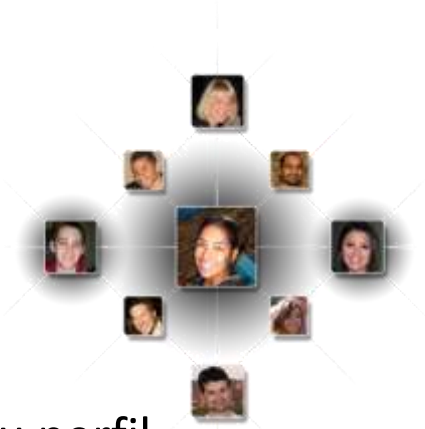


Cuidado com o que escreve

Encontro Virtual

Fonte: http://www.cellus.com.br

Redes Sociais



- Não revele demais!
- Expor seus hábitos pode ajudar um criminoso a traçar seu perfil
- Cuidado com as fotos “geotagueadas”
- Use o controle de privacidade oferecido pelas redes sociais
- Revise a política de segurança da empresa que você trabalha

Nenhuma corrente é mais forte do que o seu elo mais fraco

Final da aula

Dúvidas?

Contatos:
http://about.me/vlbarreira

Cópia da apresentação:
http://bit.ly/Unip17