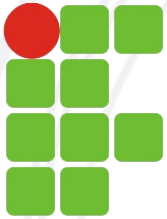


INSTITUTO FEDERAL
PIAUÍ
Campus Parnaíba

Introdução a Segurança

Prof. Msc Denival A. dos Santos

Pára-choque de caminhão

"Se você acredita que a tecnologia pode resolver os seus problemas de segurança, então é porque não conhece os seus problemas nem conhece a tecnologia."

Bruce Schneier, "SECRETS AND LIES"

Introdução

- No mundo atual a posse e o uso do conhecimento passou a ser um fator estratégico decisivo para muitas empresas e corporações. Estamos vivendo a época batizada como "Era da Informação". No entanto, ela é volátil e frágil.
- Atualmente as empresas tem seus ativos físicos e suas informações constantemente expostos a diversas ameaças, que poderiam representar prejuízos de milhares ou milhões de dólares se forem concretizadas.
- Exemplos destas ameaças são os Malware que se aproveitam de falhas na segurança dos sistemas e circulam pela Internet em busca de máquinas vulneráveis nas quais possa realizar seu ataque.
- Os fabricantes de software e a comunidade de software livre se esforçam para corrigir estas vulnerabilidades através de atualizações (patches).

Noticias pelo mundo

- *Falha shellshock afeta Mac OS X, Unix e Linux (IDGNOW, 2014).*
- *NSA espiona cidadãos da Nova Zelândia, diz Showden (O povo online, 2014).*
- *Documentos da NSA apontam Dilma Rousseff como alvo de espionagem (G1 politica, 2013).*
- *Edward Snowden não quer que você use o Dropbox (Exame.com, 2014).*
- *NSA cria projeto para vigiar qualquer dispositivo, o tempo todo (Tecmundo, 2014).*
- *Hacker expõe a intimidade de famosos em suposta falha no iCloud da apple (g1, 2014).*
- *Invasão de hackers na eleição dos EUA foi 'arma perfeita' da Rússia (Folha, 2017).*
- *Coreia do Norte pode ter ligação com ataque hacker global (Exame, 2017).*
- *Hackers podem ter usado ferramentas da inteligência dos EUA em ataque (Valor, 2017).*

Noticias pelo mundo

WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12/5/17) e colocou boa parte do mundo (incluindo o Brasil) em um caos enorme, paralisando grandes órgãos, como o Ministério Público do Estado de São Paulo (MPSP), o TJSP, o INSS e muitos outros, afetando principalmente a Europa no começo do dia.

P

Adylkuzz, ameaça foi descoberta pela empresa de segurança Proofpoint e já teria rendido milhões de dólares para cibercriminosos.

Após ataque phishing, Google aumenta a segurança no Gmail para o Android. Companhia informou que lançará um novo recurso de segurança que ajudará a identificar sites falsos que buscam enganar usuários para revelar informações pessoais

Fonte site tecmundo(www.tecmundo.com.br - 2017)

Noticias pelo mundo

Malware 'Judy' pode ter infectado até 36 milhões de smartphones Android. (2017)

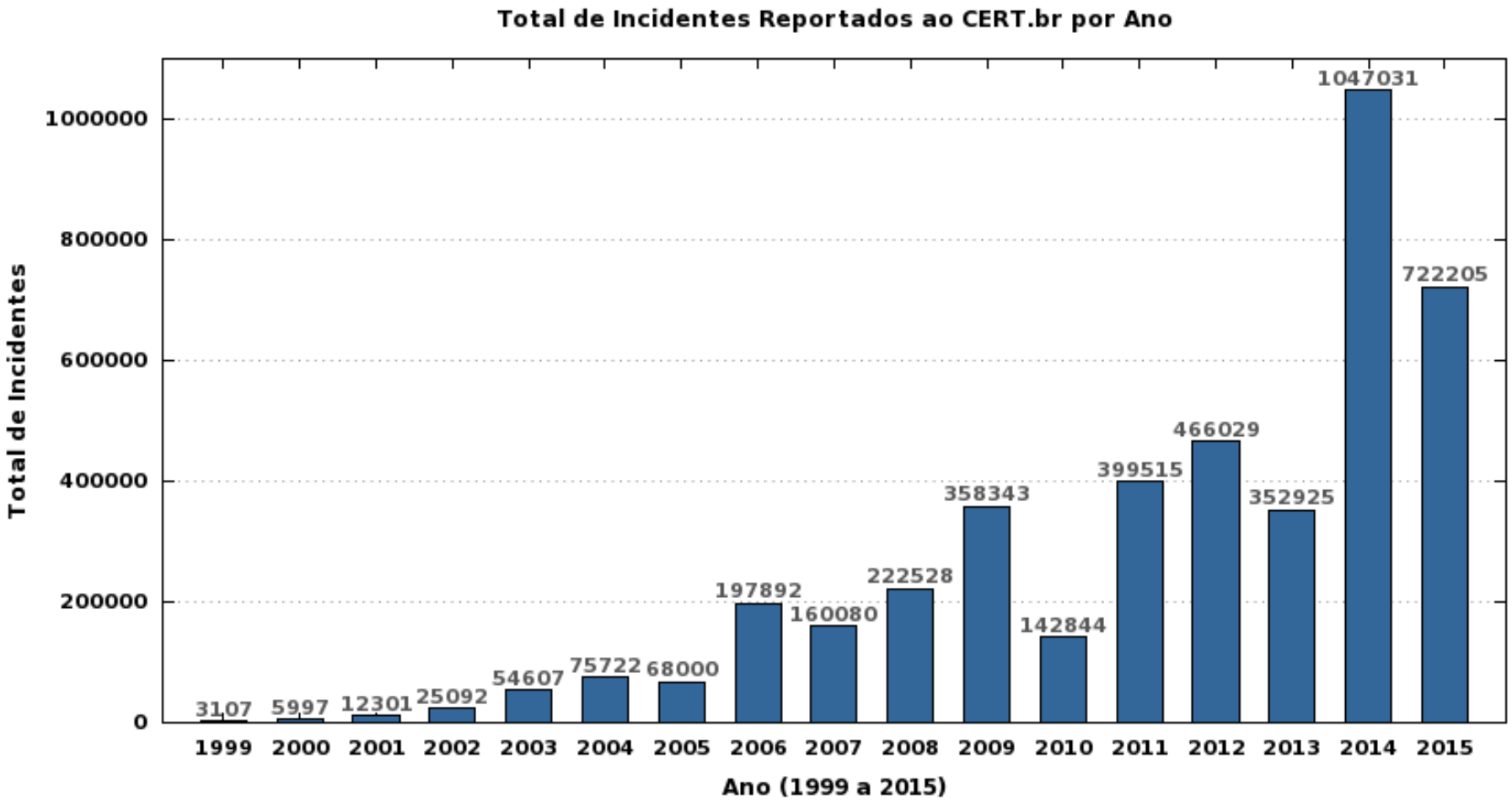
Uma grave falha de segurança presente em chips da Intel tomou conta do noticiário: a vulnerabilidade permite que um aplicativo comum tenha acesso a áreas protegidas da memória do sistema operacional, expondo informações sensíveis. Só que o problema é ainda pior: há uma brecha que também afeta processadores da AMD, da ARM e de quase todos os computadores e servidores do mundo (2018).

Malware espião Fireball já infectou mais de 24 milhões de PCs no Brasil. As informações, postadas hoje (01/6/17) no site oficial da companhia, dizem que o malware já infectou mais de 250 milhões de computadores no mundo — e mais de 24 milhões apenas no Brasil.
Os sistemas operacionais afetados são Windows e Mac OS.(2017)

Incidentes de Segurança

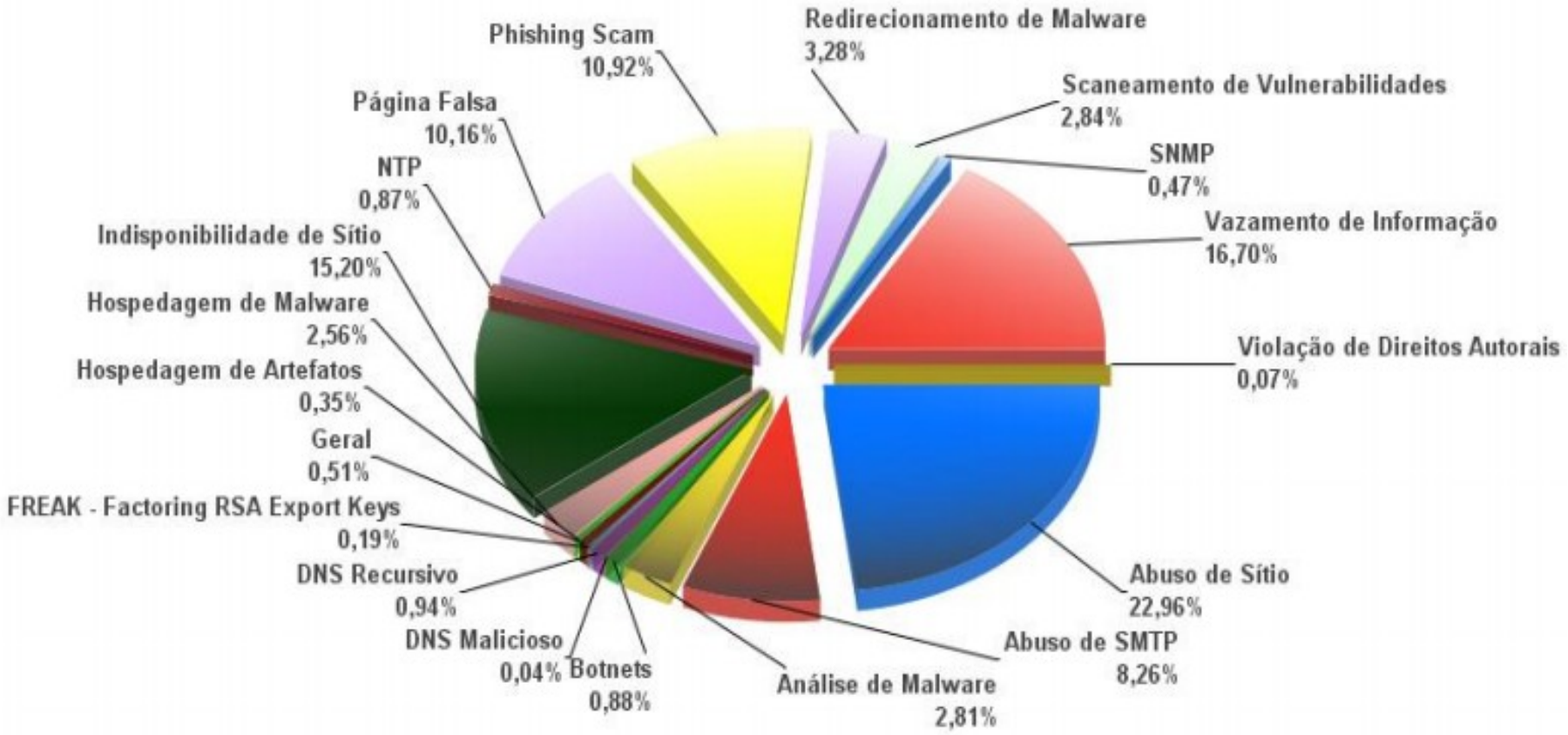
- Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: **Confidencialidade**, **Integridade** e **Disponibilidade.**
- São exemplos de incidentes de segurança
  - Tentativas de ganhar acesso não autorizado a sistemas ou dados;
  - Ataques de negação de serviço;
  - Uso ou acesso não autorizado a um sistema;
  - Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do dono do sistema;
  - Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Incidentes de Segurança: 1999 e 2015



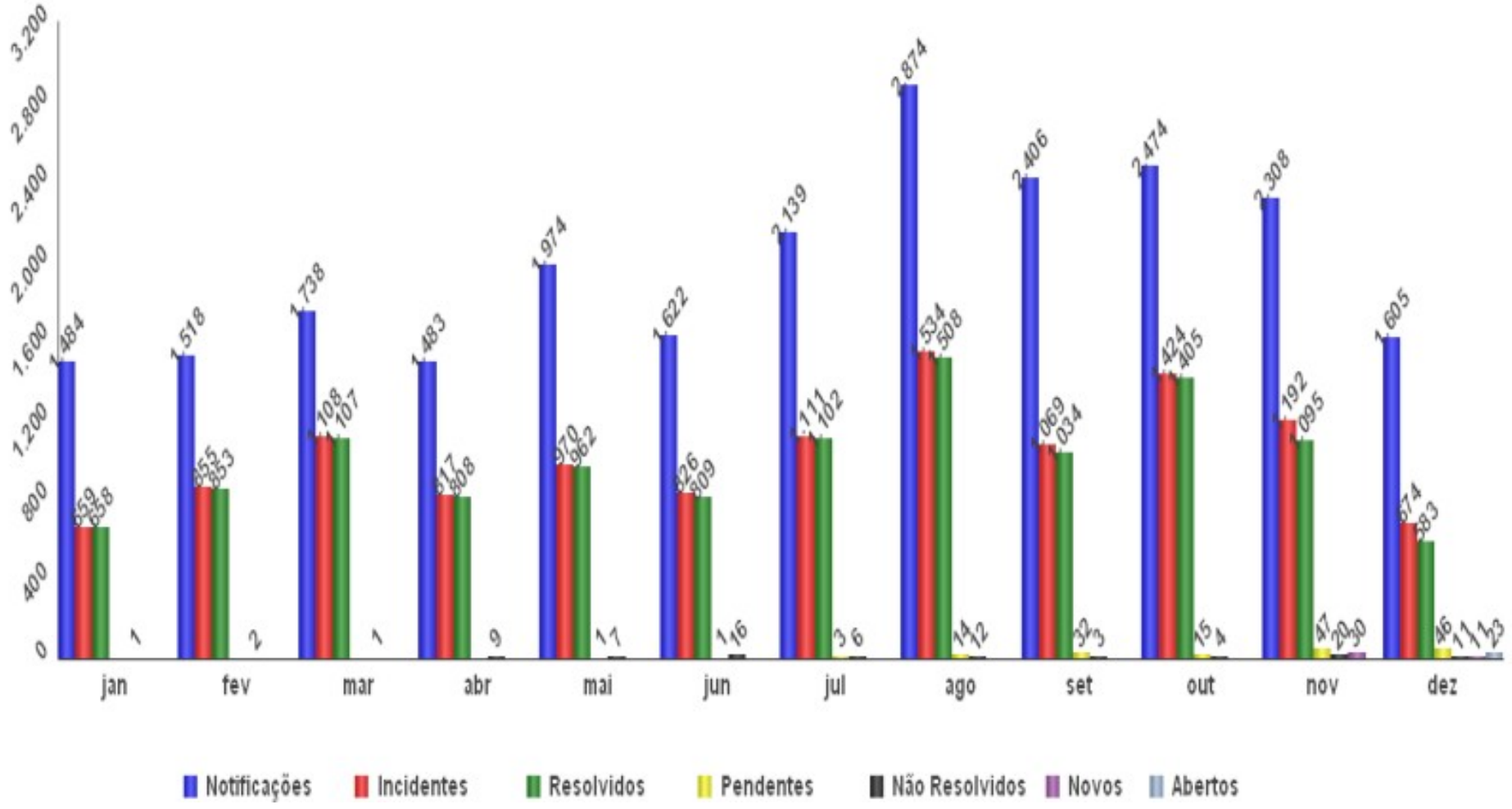
Fonte: www.cert.br

Incidentes reportados por categoria: 2016



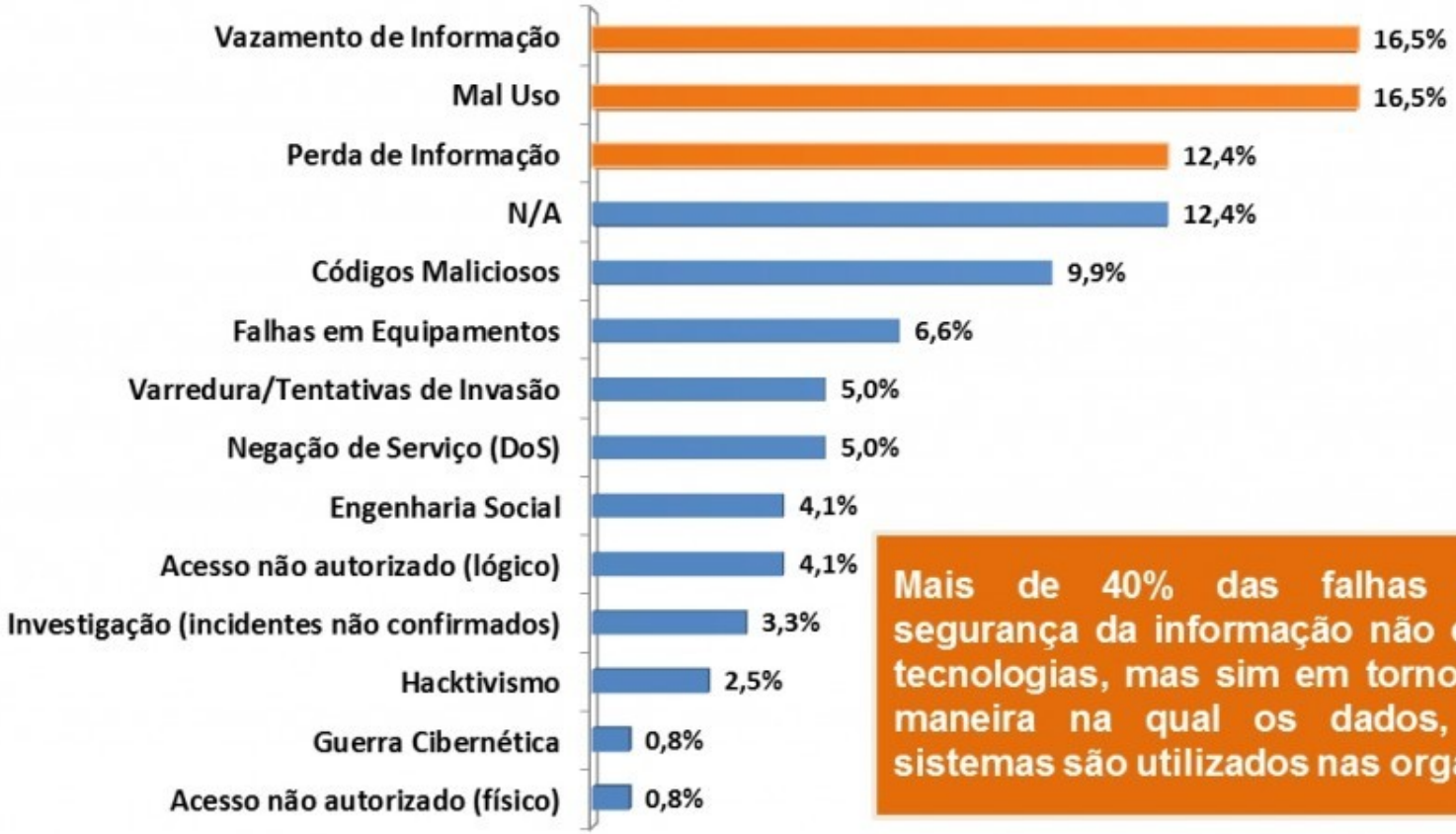
Fonte: www.ctir.gov.br

Incidentes por status e mês de criação: 2016



Fonte: www.ctir.gov.br

Os incidentes de mais frequentes



Mais de 40% das falhas relacionadas à segurança da informação não está associada à tecnologias, mas sim em torno de pessoas e a maneira na qual os dados, informações e sistemas são utilizados nas organizações.

DARYUS

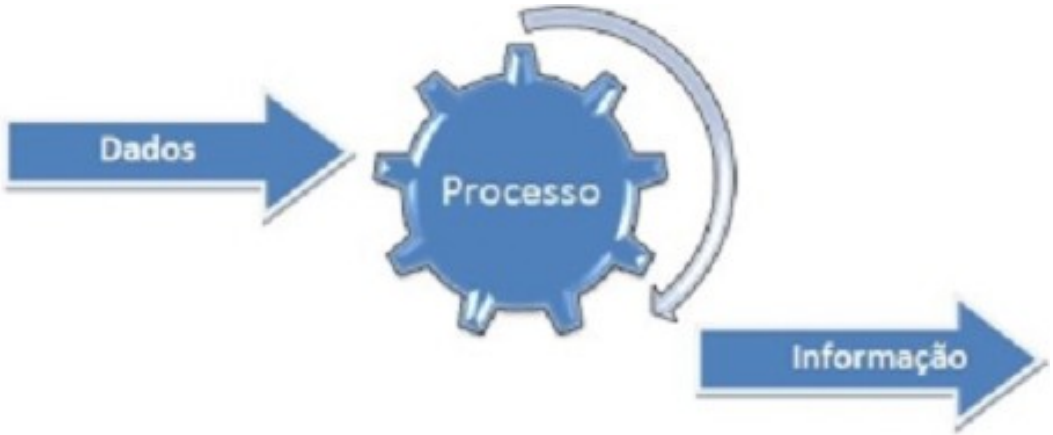
Implementação de um sistema de segurança

Podemos representar a implantação de um sistema de segurança da informação na empresa como a escalada de uma grande montanha, na qual pouco a pouco iremos subindo e passando os níveis em termos de conceitos, ferramentas e conhecimento do ambiente tecnológico da empresa. Mais tarde veremos que não basta chegar ao topo da montanha; a segurança é um processo contínuo, o chamado **ciclo de segurança**.

Informação

"A informação é um ativo que como outros ativos importantes para o negócio tem valor para a organização e por consequência necessita de ser por protegido apropriadamente."

(ISO/IEC 27000)



Segurança?

Segurança da informação na nossa empresa é ESSENCIAL!
Fazemos tantas besteiras que temos que esconder bem todas elas através de várias rotinas impenetráveis pela auditoria!

Expansão contínua da fronteiras de segurança

- As fronteiras da segurança se expandem, continuamente, na medida do avanço tecnológico. O universo de novas tecnologias evolui rapidamente e de formas até imprevisíveis. Essa evolução contínua coloca os profissionais de segurança em uma posição desconfortável, tentando estabelecer controle sobre um alvo que se move e se modifica continuamente.
- O aspecto mais curioso é que muitas das novas tecnologias à disposição dos usuários, quando utilizadas com os controles de segurança apropriados, são bastante valiosas como ferramenta de apoio aos negócios. Entretanto, quando funcionários incorporam essas tecnologias arbitrariamente em seu ambiente de trabalho, podem trazer ameaças desconhecidas à corporação. Alguns exemplos de tecnologias bastante populares utilizadas no escritório, mas que podem causar sérios danos quando usadas sem o devido cuidado ou de forma maliciosa, são:
  - Telefones celulares com câmera
  - Dispositivos de armazenamento de dados portáveis
  - Dispositivos sem fio
  - Serviços peer-to-peer e web-services

Segurança

- Existe uma piada, contada mais ou menos assim:

Um guarda de segurança que trabalha no turno da noite em uma fábrica vê um homem baixinho sair do prédio, empurrando um carrinho de mão vazio. O guarda, com uma suspeita repentina, para o homem, que pergunta por que está sendo parado. "Apenas quero ter certeza de que você não está roubando nada", diz o guarda de forma grosseira. "Confira tudo o que quiser", responde o homem, e o guarda procura, mas não encontra nada suspeito e permite que o homem vá embora. Na noite seguinte, acontece à mesma coisa. Isso se repete por algumas semanas e então o baixinho não aparece mais no portão. Passam vinte anos e o guarda, já aposentado, está sentado em um bar, quando o baixinho entra. Reconhecendo-o, o guarda aposentado se aproxima, explica quem é e oferece pagar uma bebida, se o baixinho responder a uma pergunta. O homem concorda e o guarda diz: "Tenho certeza de que você estava levando algo, mas nunca consegui descobrir o que você estava roubando". O baixinho pegou a bebida e, enquanto levava o copo à boca, disse: "Eu estava roubando ....."