INSTITUTO FEDERAL
PIAUÍ

Conceitos e Princípios

SEGURANÇA DA INFORMAÇÃO

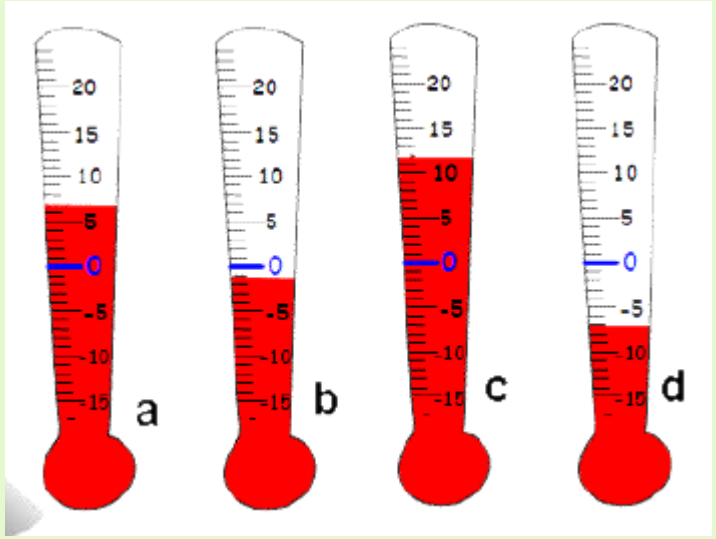
Prof. Silvino Marques
silvinomarques@ifpi.edu.br

Hierarquia DIKW

- Ciência da Informação
  - Pirâmide do conhecimento

Hierarquia DIKW

- O que é um dado?
  - É o registro de um evento
  - Fácil de representar, manipular, transportar.



Hierarquia DIKW

- O que é uma informação?
  - Conjunto de dados organizado em um contexto
  - Com significado, transmissão mais elaborada.

Hierarquia DIKW

- O que é conhecimento?
  - Informações inter-relacionadas: como usar
  - Transmissão complexa.

Hierarquia DIKW

- O que é sabedoria?
  - Conhecimento com entendimento de uso
  - Transmissão muito difícil: prática!

Importância da Informação

- Necessidades das empresas
  - ✓ Saber fazer
  - ✓ Aprimorar o que faz
  - ✓ Conhecer a quem vender
  - ✓ Satisfazer aos clientes.
- Tudo isso exige informações
  - ✓ São essenciais para os negócios!

Importância da Informação

- Informações devem ser protegidas!
  - ✓ Garantir continuidade dos negócios
  - ✓ Maximizar o retorno de investimentos/oportunidades
  - ✓ Minimizar transtornos.
- Informação em constante risco
  - ✓ Em especial porque muitas são “sensíveis”
  - ✓ Proteção dos negócios
  - ✓ Lei Geral de Proteção de Dados

Segurança da Informação

Então a SEGURANÇA DA INFORMAÇÃO, define mecanismos para garantir a proteção das mesmas.

Princípios da Segurança da Informação

A segurança da informação tem vários aspectos importantes, sem dúvida três deles se destacam.

1) CONFIDENCIALIDADE

- Capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizados, a vejam.

Confidencialidade

- Atualmente, obter confidencialidade é mais desafiador.
- Computadores estão em todos os lugares e cada um é capaz de executar operações que podem comprometer este principio.
- A seguir veremos alguns conceitos utilizados para proteger informação sensível:

Confidencialidade

- *Encriptação*
  - ✓ transformação de informação usando um segredo (chave de encriptação), de modo que essa informação transformada possa apenas ser lida usando outro segredo (chave de decriptação);
- *Controle de acesso*
  - ✓ regras e políticas que limitam o acesso a informação confidencial apenas para aquelas pessoas e/ou sistemas com uma "necessidade de saber".
- *Autenticação*
  - ✓ a determinação da identidade ou do papel de alguém.

Princípios da Segurança da Informação

2) INTEGRIDADE

- A informação deve estar correta, ser verdadeira e não está corrompida.

Integridade

- Existem diversas maneiras pelas quais a integridade dos dados pode ser comprometida em um sistema de computação e em redes, e esses comprometimentos podem ser **benignos** ou **maliciosos**;
- Existem várias ferramentas especialmente projetadas para apoiar a integridade, incluindo as seguintes:

Integridade

- *Cópias de segurança*
  - ✓ o arquivamento periódico de dados;
- *Somas de verificação (checksums)*
  - ✓ a computação de uma função que mapeia o conteúdo de um arquivo para um valor numérico.
- *Códigos de correção de dados*
  - ✓ métodos para armazenar dados de tal maneira que pequenas alterações podem ser facilmente detectadas e automaticamente corrigidas.

Princípios da Segurança da Informação

3) DISPONIBILIDADE

- A informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais ou pessoais.

Disponibilidade

- A qualidade de uma informação é diretamente associada à sua disponibilidade;
- Portanto, assim como para confidencialidade e integridade, pesquisadores em segurança de computadores e projetista de sistemas desenvolveram diversas ferramentas para providenciar disponibilidade, incluindo as seguintes:

Disponibilidade

- *Proteções físicas*
  - ✓ infraestrutura projetada para manter a informação disponível mesmo na presença de desafios físicos;
- *Redundâncias computacionais*
  - ✓ computadores e dispositivos de armazenamento que servem como reserva no caso de falhas;

Segurança da informação

Segurança da Informação

- Além destes três aspectos principais, temos:
  - ✓ AUTENTICAÇÃO – Garantia que o usuário é quem de fato diz ser;
  - ✓ AUTORIZAÇÃO – Processo de concessão de direitos a uma entidade autenticada;
  - ✓ AUDITORIA – Capacidade de detectar fraudes.
  - ✓ NÃO REPÚDIO – Capacidade do sistemas de provar que o usuário executou uma determinada ação;
  - ✓ LEGALIDADE – Estar dentro das leis vigentes;
  - ✓ PRIVACIDADE – Condição do que é pessoal, íntimo, relacionado a vida privada.

Incidente de Segurança

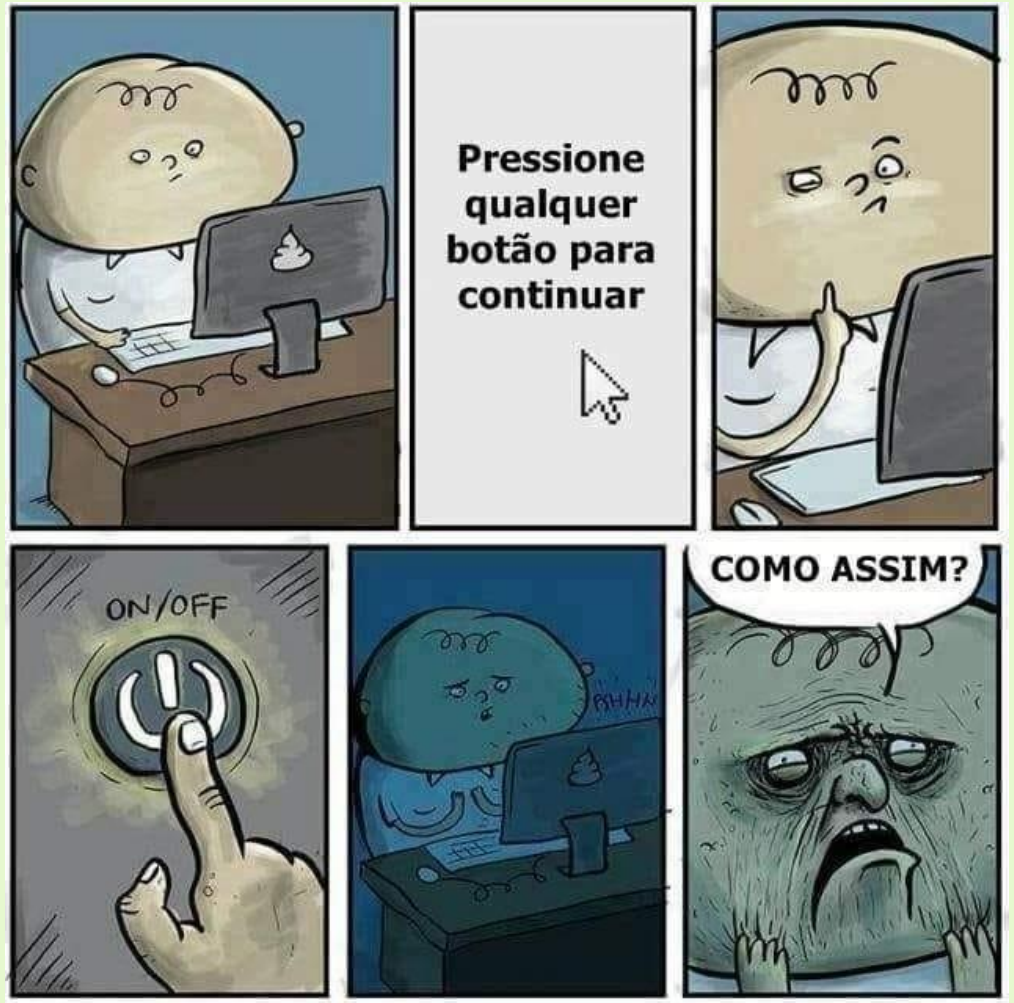
É a ocorrência de um evento que possa causar interrupções nos processos de negócio em consequência da violação de algum dos aspectos listados anteriormente.

Incidente de Segurança

- Outros fatores, relacionados a natureza, greves, manifestações, etc., também podem gerar um incidente de segurança.
- Pois afetam a disponibilidade e a integridade da informação.

Incidente de Segurança

Outra classe de problemas de segurança ocorre devido à **má operação**, **operação incorreta** ou **ataque ao sistema**.



Ativo de Informação

A informação é um bem de grande valor para os processos de negócios da organização, mas também devemos considerar a **tecnologia**, o **meio** que a suporta, que a mantém e que permite que ela exista, as **pessoas** que a manipulam e o **ambiente** onde ela está inserida.

Assim podemos descrever que **ativo da informação é composto pela informação e tudo aquilo que a suporta ou se utiliza dela.**

Ativo de Informação

INFORMAÇÃO
O PRINCIPAL ATIVO
DE UM NEGÓCIO

A gestão de dados tornou-se o ponto crucial para a sobrevivência das instituições, mas poucas mantém programas de treinamento sobre a mesma.

Ataque

- Um tipo de incidente de segurança caracterizado pela existência de um agente que busca obter algum tipo de retorno, atingindo algum ativo de valor.

Vulnerabilidade

- Os ativos de informação possuem vulnerabilidades que podem ser exploradas por um agente que poderá realizar um ataque,
- Essas vulnerabilidades são o PONTO FRACO, da segurança do ativo.

Ameaça

- É um ataque potencial a um ativo da informação. É um agente externo que, aproveitando das vulnerabilidades, poderá quebrar um ou mais dos três princípios da segurança da informação.

Impacto

- O impacto de incidente de segurança é medido pelas consequências que possa causar aos processos de negócio suportados pelo ativo em questão.
- Os ativos possuem valores diferentes, pois suportam informações com relevância diferentes para o negócio da organização, quanto maior o valor do ativo, maior será o impacto de um incidente.

Impacto

- De acordo com a proporção do impacto algumas empresas podem perder informações sobre patentes, processos industriais e outros.

Controle

- Percebemos o quão vulnerável a informação pode ser, e a quantidade de agentes que estão buscando obter os ativos de um empresa.
- Assim, controle é todo e qualquer mecanismo utilizado para diminuir fraquezas (vulnerabilidades) de um ativo da informação, seja um equipamento, tecnologia, pessoa ou processo.

Novos desafios para Segurança

- Tecnologias sem fio;
- Dispositivos móveis;
- Internet das Coisas;
- Cidades Inteligentes;
- Redes sociais;
- Computação em nuvem;

Tendências da Segurança

- Era de ouro do *hacking*?
- Adoção rápida de novas técnicas e tecnologias, muitas delas não testadas;
- Grande número de vulnerabilidades;
- Informações amplamente disponíveis para o aprendizado.

Tendências da Segurança – Cenário Pessimista

- O expertise dos hackers está aumentando;
- A sofisticação dos ataques e das ferramentas de ataque está aumentando;
- A efetividade das invasões está aumentando;
- O número de invasões está aumentando;
- O número de usuários da Internet está aumentando;
- A complexidade dos protocolos, das aplicações e da rede está aumentando;
- O ciclo de desenvolvimento e testes de software está diminuindo;
- Softwares com vulnerabilidades, algumas repetidas, continuam sendo desenvolvidos.

Tendências da Segurança – Cenário Otimista

- Desenvolvimento de software com preocupação com a segurança;
- Projetos de rede com preocupação com a segurança;
- Segurança fazendo parte de qualquer aspecto da tecnologia, assim como a qualidade faz parte de produtos e processos.

Ou quem sabe?

Referências Bibliográficas

Introdução a Segurança de Computadores – Michael T. GOODRICH, Roberto TAMASSIA. Porto Alegre, RS, Brasil. 2013.

Segurança de Redes em Ambientes Cooperativos – Emilio T. NAKAMURA, Paulo L. GEUS. São Paulo, SP, Brasil. 2007.