



Codificação de Segurança da informação

Conceitos de Segurança

Prof. Me. Gabriel Caixeta Silva

A informação

- ❖ Eras da humanidade.
 - ❖ Revolução industrial.
 - ❖ 14/07/1789 Tomada da Bastilha.
 - ❖ Revolução da informação.
 - ❖ Em 1994 menos de 3%.
 - ❖ Desde 2006 as exportações de bens intangíveis superaram os bens tangíveis.

A informação

- ❖ As informações são portanto o principal patrimônio de uma organização.
- ❖ A informação é portanto um ponto crucial para a sobrevivência da organização.
- ❖ Evolução:
 - ❖ Papel: trancar a sala e restringir o acesso.
 - ❖ Mainframes centralizados: controles lógicos.
 - ❖ E agora ? Computadores pessoais, redes, descentralização ...

A informação

- ❖ Qualquer um pode invadir um computador ... Só depende de conhecimento.
- ❖ Usuário mais consciente.
- ❖ Não importa se foi um funcionário insatisfeito que apagou o dado, se foi um vírus, falha de hardware ou sobrecarga elétrica. O que importa é que o dado foi adulterado ou perdido.

A informação

- ❖ Ambientes controlados:
 - ❖ Desastres naturais.
 - ❖ Incêndio, terremoto, enchente.
 - ❖ Falhas estruturais.
 - ❖ Energia elétrica, falha ar condicionado.
 - ❖ Sabotagem, fraudes, acessos não autorizados.
 - ❖ Cracker, espionagem industrial.

Segurança

- ❖ A **proteção** de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a **reduzir** a **probabilidade** e o **impacto** de incidentes de segurança.

Confidencialidade

- ❖ O mesmo que privacidade.
- ❖ Proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação.

Integridade

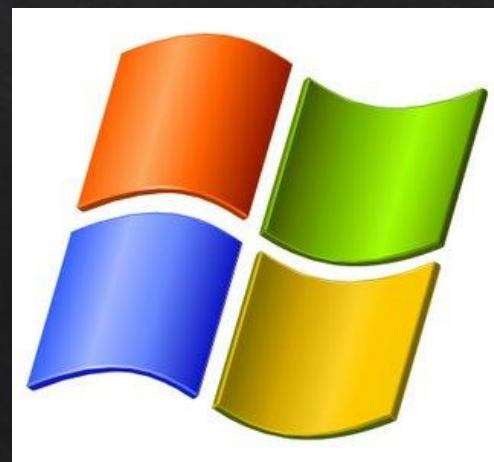
- ❖ Evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação.
- ❖ Dados neste contexto engloba dados, programas, documentação, registros ...
- ❖ Enquanto o objetivo da confidencialidade está mais voltado á leitura de dados, a integridade preocupa-se mais com a gravação e alteração de dados.

Disponibilidade

- ❖ Proteger serviços de informática de tal forma que não sejam degradados ou tornado indisponíveis sem a devida autorização.
- ❖ Para um usuário autorizado, um sistema não disponível quando se necessita dele pode ser tão ruim OU PIOR que um sistema inexistente.
- ❖ Engloba equipamentos tolerantes a falhas.
- ❖ DoS.

Consistência

- ❖ Certificar-se de que o sistema atua de acordo com as expectativas dos usuários autorizados.
- ❖ Por causa de um bug no editor de textos, o arquivo É apagado e o usuário perde todos os seus dados ...



Isolamento ou uso legítimo

- ❖ Regular o acesso ao sistema.
- ❖ O acesso não autorizado é sempre um problema, pois alem de ser necessário identificar quem acessou e como, é preciso certificar de que nada importante do sistema foi adulterado ou apagado.
- ❖ Custo de reconstrução e recuperação.

Auditoria

- ❖ Proteger os sistemas contra erros e atos maliciosos cometidos por usuários autorizados.
- ❖ Identificar os autores e suas ações:
 - ❖ Trilhas de auditoria e logs.
 - ❖ O que foi alterado, por quem e quando.
 - ❖ Em alguns casos pode ser possível recuperar o estado original.



Auditoria

- ❖ O principal É evitar eventos indesejados.
- ❖ Na prática, nem todas podem ser evitadas.
- ❖ Para lidar com essas situações, É necessário monitorar as ações dos usuários, detectar falhas de segurança e ser capaz de responsabilizar os culpados.



Confiabilidade

- ❖ Garantir que, mesmo em condições adversas, o sistema atuará conforme o esperado.
- ❖ Ex: Onde a confiabilidade É o objetivo de segurança mais importante:
 - ❖ Sistemas de energia nuclear, de controle de tráfego aéreo e de controle de vôo.

Como escolher ...

- ❖ Apesar de todos os objetivos serem importantes, dependendo do tipo da organização, alguns são mais importantes do que outros.
- ❖ Ex: Em sistemas bancários integridade e auditoria são aspectos mais relevantes, seguidos de privacidade e disponibilidade.

Perguntas ...

- ❖ O que se quer proteger ?
- ❖ Contra o que ou quem ?
- ❖ Quais são as ameaças mais prováveis ?
- ❖ Qual a importância de cada recurso ?
- ❖ Qual o grau de proteção desejado ?
- ❖ Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados ?

Perguntas ...

- ❖ Quais as expectativas dos usuários e clientes em relação a segurança de informações ?
- ❖ Quais as consequências para a instituição se seus sistemas e informações forem corrompidos ou roubados ?

Definições

- ❖ Recurso.
 - ❖ Pode ser físico, software, hardware ou informação.
- ❖ Ameaça.
 - ❖ Evento ou atitude indesejável(roubo, incêndio, vírus, etc.).
- ❖ Vulnerabilidade.
 - ❖ Fraqueza ou deficiência que pode ser explorada por uma ameaça.

Definições

- ❖ Ataque.
 - ❖ Ameaça concretizada.
- ❖ Impacto.
 - ❖ Conseqüência de uma vulnerabilidade do sistema ter sido explorada por uma ameaça.
- ❖ Probabilidade.
 - ❖ Chance de uma ameaça atacar com sucesso o sistema computacional.

Definições

- ❖ Risco.
 - ❖ Medida da exposição a qual o sistema computacional está sujeito.
 - ❖ Depende da probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque.
 - ❖ Ameaças, vulnerabilidades associadas e impacto.

Ameaças

- ❖ Vazamento de informações.
 - ❖ Voluntário ou involuntário.
 - ❖ A informação tem valores diferentes:
 - ❖ Uma indústria pode quebrar.
 - ❖ Um hospital ou banco pode enfrentar problemas na justiça.
- ❖ Violação de integridade.
 - ❖ Comprometimento dos dados.

Ameaças

- ❖ Indisponibilidade.
- ❖ Acesso e uso não autorizado.
 - ❖ Comprometimento dos dados.

Após o ataque

- ❖ Mascaramento.
 - ❖ Uma entidade (pessoa ou programa) se faz passar por outra entidade.
- ❖ Desvio de controles.
 - ❖ Burla outros controles para obter outros direitos de acesso.

Após o ataque

- ❖ Violação autorizada
 - ❖ Um usuário ou programa autorizado usa o sistema com propósitos não autorizados.
- ❖ Ameaças programadas.
 - ❖ Código de software que se alojam no sistema com intuito de comprometer a segurança.
 - ❖ Ex: rootkit, trojan, backdoor ...

Dados

- ❖ Causas mais comuns:
 - ❖ 81% funcionários.
 - ❖ 13% pessoas externas a organização.
 - ❖ 6% ex-funcionários.

Dados

- ❖ Danos mais comuns:
 - ❖ 52% erros humanos.
 - ❖ 15% incêndios.
 - ❖ 10% atividades desonestas.
 - ❖ 10% sabotagem.
 - ❖ 10% água.
 - ❖ 3% terrorismo.