AUDITORIA EM SISTEMAS E SEGURANÇA DA INFORMAÇÃO

Professor Me. Vladimir Geraseev Junior

Fatec Centro Paula Souza Governo de São Paulo

Curso: TECNOLOGIA EM DEFESA CIBERNÉTICA

Disciplina: Auditoria em sistemas e segurança da informação

Sejam Bem Vindos!

Prof. Vladimir Geraseev Junior

PROF VLADIMIR GERASEEV JUNIOR

- **GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO**
- **MESTRADO EM ENGENHARIA - UNITAU**

- EXPERIÊNCIA PROFISSIONAL:

- COMPANHIA DE INFORMÁTICA DE JUNDIAÍ – ARQUITETO DE REDES
- EMBRAER – GRUPO DE ENGENHARIA
- INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS – INPE – ANALISTA DE REDES E SEGURANÇA
- IMPLEMENTAÇÃO DOS REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES (ATO 77) – ANATEL
- CONSULTORIA EM CONDUÇÂO DE PENTESTS

PROF VLADIMIR GERASEEV JUNIOR

- EXPERIÊNCIA PROFISSIONAL ACADÊMICA.

- PROFESSOR NA FATEC TAUBATÉ
- PROFESSOR NA ETEC JACAREÍ
- PROFESSOR EM UNIVERSIDADES PARTICULARES (UNIP, UNIVAP, FAPI)

EMENTA DA DISCIPLINA

- Requisitos de segurança de aplicações, de base de dados e de comunicações.
- Políticas de segurança.
- Criptografia.
- Firewalls.
- Vulnerabilidades e principais tecnologias de segurança.

EMENTA DA DISCIPLINA

- Metodologia de auditoria em Tecnologia da Informação. Análise de riscos.
- Revisão e avaliação de sistemas e de recursos de tecnologia de informação.
- Métodos e técnicas de auditoria de sistemas e de T.I.
- Documentação: papéis de trabalho, Relatórios de Auditoria e Pareceres

OBJETIVOS DA DISCIPLINA

- Compreender e aplicar as melhores práticas de Segurança da Informação de acordo com normas e padrões conhecidos no mercado de Tecnologia da Informação;
- Entender e aplicar as melhores metodologias destinadas a Auditoria de sistemas de informação, redes de computadores;
- Conceituar procedimentos de prevenção e identificação de invasão em sistemas;
- Entender processos referentes a auditoria de sistemas sobre o aspecto da segurança de informação

BIBLIOGRAFIA BÁSICA

- FERREIRA, F N; ARAUJO, M. **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**. CIÊNCIA MODERNA, 2008.
- FONTES, E. **PRATICANDO A SEGURANÇA DA INFORMAÇÃO**. BRASPORT, 2008.
- STALLINGS, W. **CRIPTOGRAFIA E SEGURANÇA DE REDES**. 4 ED. SÃO PAULO: PEARSON, 2008.

BIBLIOGRAFIA COMPLEMENTAR

- SCHMIDT, PAULO; SANTOS, JOSÉ L.; ARIMA, CARLOS H. **FUNDAMENTOS DE AUDITORIA DE SISTEMAS**. SP: ATLAS, 2006.
- GIL, ANTÔNIO DE LOUREIRO. **AUDITORIA DE COMPUTADORES**. 5.ED. SÃO PAULO: ATLAS, 2000.
- ARAÚJO, MÁRCIO TADEU DE; FERREIRA, FERNANDO NICOLAU FREITAS. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: **GUIA PRÁTICO PARA ELABORAÇÃO E IMPLEMENTAÇÃO.** 2. ED. SÃO PAULO: CIÊNCIA MODERNA LTDA, 2008.
- PEIXOTO, M C P. **ENGENHARIA SOCIAL E SEGURANÇA DA INFORMAÇÃO**. BRASPORT, 2006.

SEGURANÇA DA INFORMAÇÃO

É A PROTEÇÃO DAS INFORMAÇÕES, SISTEMAS, RECURSOS E DEMAIS ATIVOS CONTRA DESASTRES, ERROS(INTENCIONAIS OU NÃO), MANIPULAÇÃO NÃO AUTORIZADA E PROTEÇÃO DE VÁRIOS TIPOS DE AMEAÇAS PARA GARANTIR A CONTINUIDADE DO NEGÓCIO.

INTRODUÇÃO

A informação é algo que contém um significado e causa impacto em diferentes graus, tornando-a o elemento chave da extração e criação do conhecimento. O conhecimento só poderá ser formado quando o indivíduo for exposto à informação, deste modo é possível afirmar que poderá até haver informação sem conhecimento, mas não conhecimento sem informação.

DADO

E QUALQUER ELEMENTO IDENTIFICADO EM SUA FORMA BRUTA QUE, POR SI SÓ, NÃO CONDUZ UMA COMPREENSÃO DE UM DETERMINADO FATO OU SITUAÇÃO.

“DADOS SÃO ÁTOMOS DA INFORMAÇÃO ”

EX: 1024

INFORMAÇÃO

SÃO OS RESULTADOS DOS DADOS DEVIDAMENTE TRATADOS, COMPARADOS, CLASSIFICADOS, RELACIONÁVEIS ENTRE OUTROS DADOS SERVINDO PARA TOMADAS DE DECISÕES .

“SÃO OS DADOS TRABALHADOS, GERANDO A INFORMAÇÃO”

EX: **1024 CLIENTES ATIVOS**

CONHECIMENTO

É O CONJUNTO DE FERRAMENTAS CONCEITUAIS E CATEGORIAS USADA PARA CRIAR, COLECIONAR, ARMAZENAR E COMPARTILHA A INFORMAÇÃO.

“SÃO AS INFORMAÇÕES TRABALHADAS ”

VALOR DA INFORMAÇÃO.

O VALOR DA INFORMAÇÃO É DETERMINADO PELO QUE A ORGANIZAÇÃO OU USUÁRIO DÁ À ELA.

INTRODUÇÃO

No mundo atual a posse e o uso do conhecimento passou a ser um fator estratégico decisivo para muitas empresas. Estamos vivendo a época batizada como "Era da Informação". Mas a informação é volátil, frágil. Hoje, ela pode desaparecer na velocidade de um pulso elétrico.

Atualmente, as informações constituem o objeto de maior valor para as empresas. Por esse e outros motivos a segurança da informação é um assunto tão importante para todos, pois afeta diretamente todos os negócios de uma empresa ou de um indivíduo.

Importância da Informação para o Negócio - A informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio.

CONCEITOS

- **Ativo de Informação:** Qualquer elemento que tenha valor para uma organização.
- **Valor do Ativo:** Quantificação de perda de determinado ativo quando esse tem sua confidencialidade, integridade ou disponibilidade (Princípios Básicos da SI) afetadas.
- **Vulnerabilidade:** Falha no ambiente que ameace algum ativo.
- **Ameaça:** Possibilidade de exploração de uma vulnerabilidade.
- **Impacto:** Resultado da concretização de uma ameaça contra a vulnerabilidade de um ativo.

ATIVOS DE INFORMAÇÃO

- A segurança da informação tem como propósito proteger as **INFORMAÇÕES,** sem importar onde estejam situadas.

- Um sistema de segurança da informação tem por objetivo proteger e controlar os **ATIVOS DE INFORMAÇÃO,** garantindo os três princípios básicos da segurança da informação.

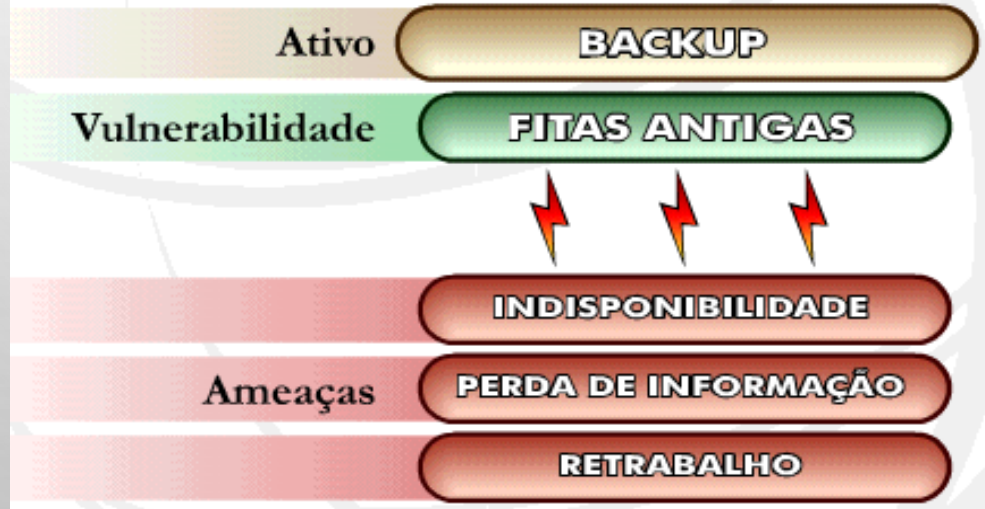
ATIVOS DE INFORMAÇÃO

CLASSIFICAÇÃO DE ATIVOS	
INFORMAÇÕES	
EQUIPAMENTOS E SISTEMAS	SOFTWARE HARDWARE ORGANIZAÇÃO
PESSOAS	

ATIVOS DE INFORMAÇÃO

Ativos

Exemplo de Ativo:



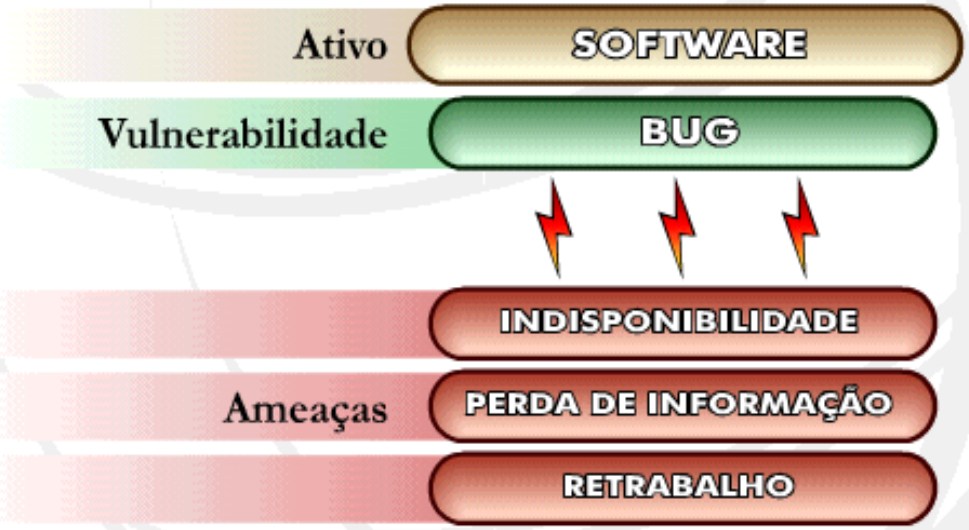
Após um longo período de uso as mídias utilizadas no Backup começam a se degradar diminuindo assim a capacidade de armazenar informação.

Você já verificou a data de validade recomendada pelo fabricante de suas fitas de Backup?

ATIVOS DE INFORMAÇÃO

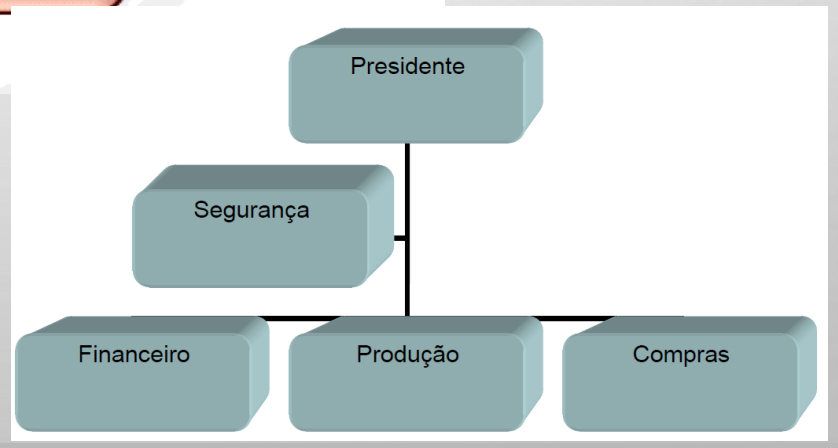
1 Ativos

Exemplo de Ativo:

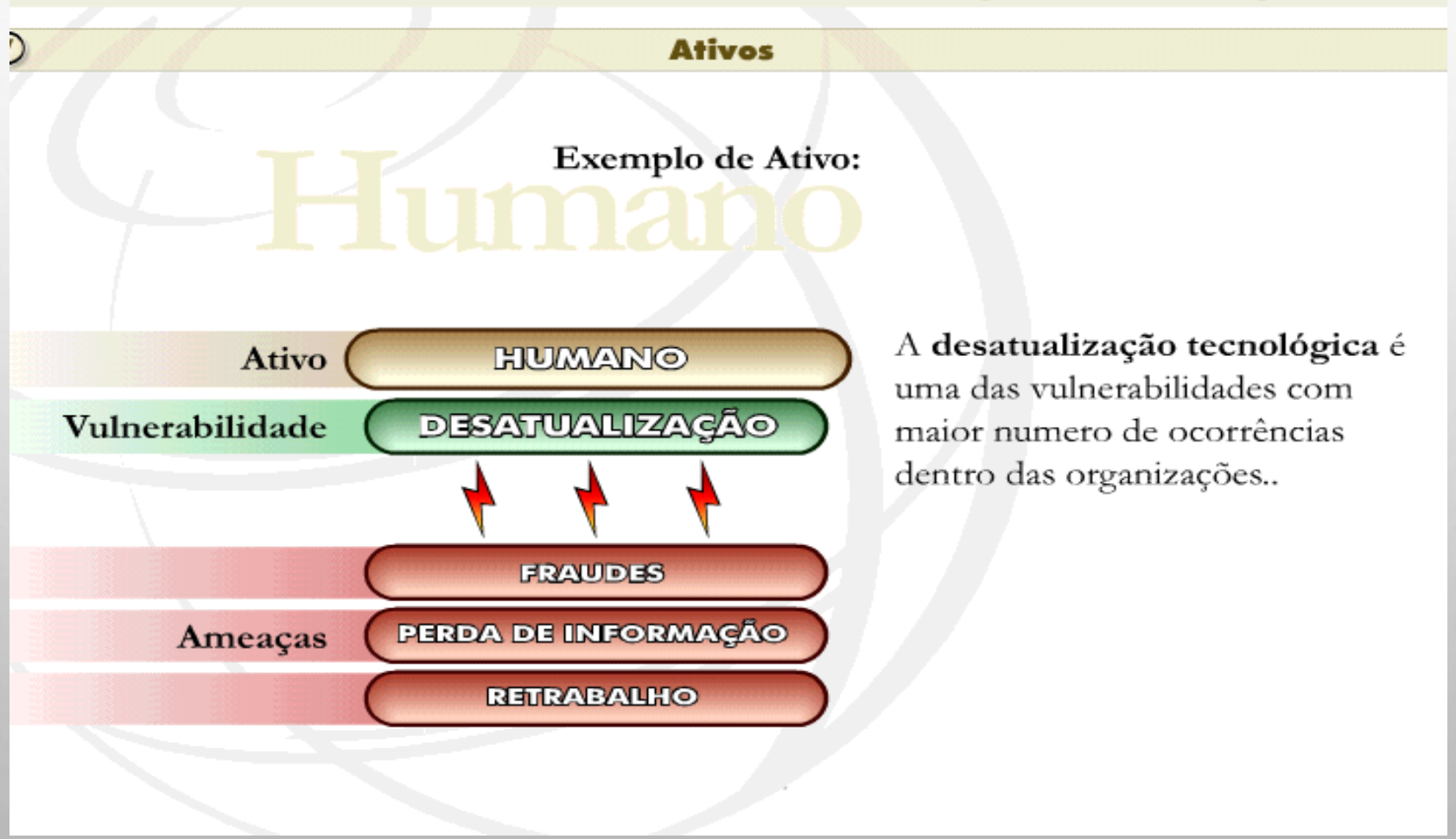


Este exemplo representa um software com uma vulnerabilidade muito comum que é um **Bug**. Este erro submete o ativo a diversas ameaças tais como: a Indisponibilidade, Perda de Informação, Retrabalho.

ATIVOS DE INFORMAÇÃO



ATIVOS DE INFORMAÇÃO



PRINCÍPIOS BÁSICOS

- Existem três* princípios básicos da segurança da informação, são eles:

- **Disponibilidade**
- **Confidencialidade**
- **Integridade**

* Existem autores que destacam mais de três, são eles: Autenticidade, Não repúdio, Legalidade, Privacidade e Auditoria

DISPONIBILIDADE

- A informação está acessível à pessoas autorizadas sempre que necessário.

QUEBRA DE DISPONIBILIDADE

- Sistemas fora do ar
- Ataques de Negação de Serviço
- Perdas de Documentos
- Perda de Acesso à informação

DISPONIBILIDADE

- OS RECURSOS DEVEM ESTAR DISPONÍVEIS PARA OS USUÁRIOS AUTORIZADOS QUANDO SOLICITADOS.
- QUALIDADE DE SERVIÇO PODE SER FUNDAMENTAL PARA UM NEGÓCIO.

CONFIDENCIALIDADE

Somente Pessoas explicitamente autorizadas podem ter acesso à informação.

QUEBRA DE CONFIDENCIALIDADE

- Conversas no elevador, restaurantes, etc. sobre assuntos confidenciais de trabalho, disponibilizando assim a informação para todos à sua volta.

- Engenharia Social

CONFIDENCIALIDADE

- RECURSOS OU INFORMAÇÃO PODEM SER ACESSADOS APENAS POR USUÁRIOS AUTORIZADOS.
- REQUER IDENTIFICAÇÃO DE USUÁRIO (AUTENTICAÇÃO) E CONTROLE DE PERMISSÕES DE ACESSO (AUTORIZAÇÃO),
- AS PERMISSÕES PARA UM MESMO USUÁRIO PODEM DEPENDER DE LOCALIZAÇÃO FÍSICA, TEMPO OU PAPEL FUNCIONAL.

INTEGRIDADE

A informação acessada é completa, sem alterações ou distorções, e portanto, confiável. Mesmo estando errada.

QUEBRA DE INTEGRIDADE

- Falsificação de documentos
- Alteração de registro no BD

INTEGRIDADE

- RECURSOS PODEM SER MODIFICADOS APENAS POR USUÁRIOS AUTORIZADOS.
- SEGURANÇA DE TRANSAÇÕES.
- GARANTIR QUE UMA OPERAÇÃO FOI EFETUADA DA FORMA CORRETA.
- AS MODIFICAÇÕES INCLUEM CRIAR CONTEÚDO NOVO, MUDAR CONTEÚDO, MUDAR STATUS, APAGAR, ETC.

ACCOUNTABILITY

- IMPUTAÇÃO DE RESPONSABILIDADE. TER CONTROLE SOBRE OS ITENS DE SUA RESPONSABILIDADE. SER RESPONSÁVEL PELAS SUAS AÇÕES.

AUTENTICIDADE E NÃO REPUDIAÇÃO

- O SISTEMA COMPUTACIONAL DEVE SER CAPAZ DE VERIFICAR A IDENTIDADE DE UM USUÁRIO.
- O AUTENTICIDADE DO SISTEMA COMPUTACIONAL DEVERÁ SER VERIFICADA.
- NÃO REPUDIAÇÃO: UMA INFORMAÇÃO ESTÁ LIGADA AO AUTOR. O AUTOR NÃO PODE NEGAR A AUTORIA.

AUDITABILIDADE

- POSSIBILIDADE DE RASTREAR OU AUDITAR OPERAÇÕES EXECUTADAS POR USUÁRIOS E OPERADORES DO SISTEMA.

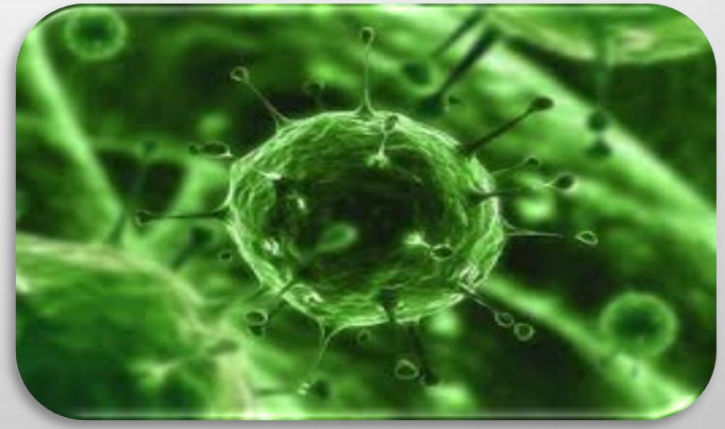
VULNERABILIDADES

São fraquezas inerentes aos ativos de informação que podem ser exploradas por ameaças ocasionando um incidente de segurança da informação. É possível que um ativo de informação possua uma vulnerabilidade que, de fato, nunca será efetivamente explorada por uma ameaça.

SISTEMA IMUNOLÓGICO FRACO

AMEAÇAS

São agentes externos ao ativo de informação que, exploram as vulnerabilidades pra gerar a quebra de um ou mais dos três princípios básicos da segurança da informação (confidencialidade, integridade e disponibilidade), ou seja, um incidente de segurança da
informação.



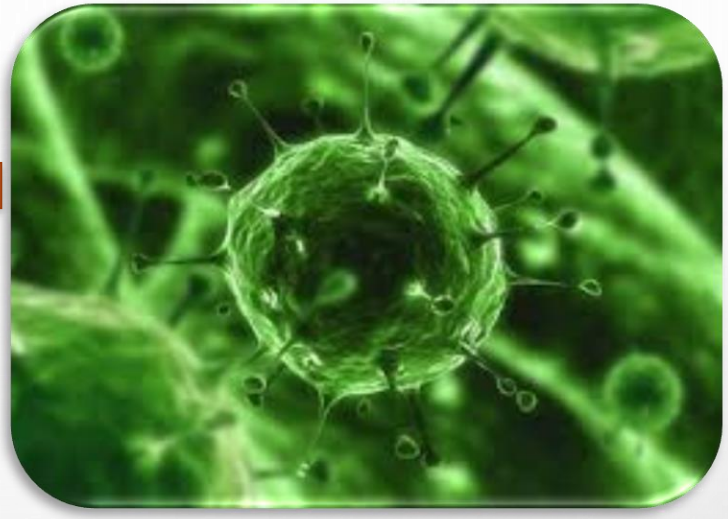
VÍRUS

INCIDENTES

Um incidente de segurança da informação é a ocorrência de um evento que possa interromper os processos do negócio de um ou mais dos três princípios básicos de segurança da informação (confidencialidade, integridade e disponibilidade).

INCIDENTE

+



VULNERABILIDADE **AMEAÇA**

=

INCIDENTE

PROBABILIDADE

Probabilidade é a chance que um incidente de segurança da informação tem de acontecer, considerando o grau das vulnerabilidades presentes nos ativos de informação e o grau das ameaças que possam explorar essas vulnerabilidades. Mas esses graus são relativos, ou seja, mesmo as mais baixas vulnerabilidades poderão representar probabilidades consideráveis, se o grau da ameaça for muito grande.

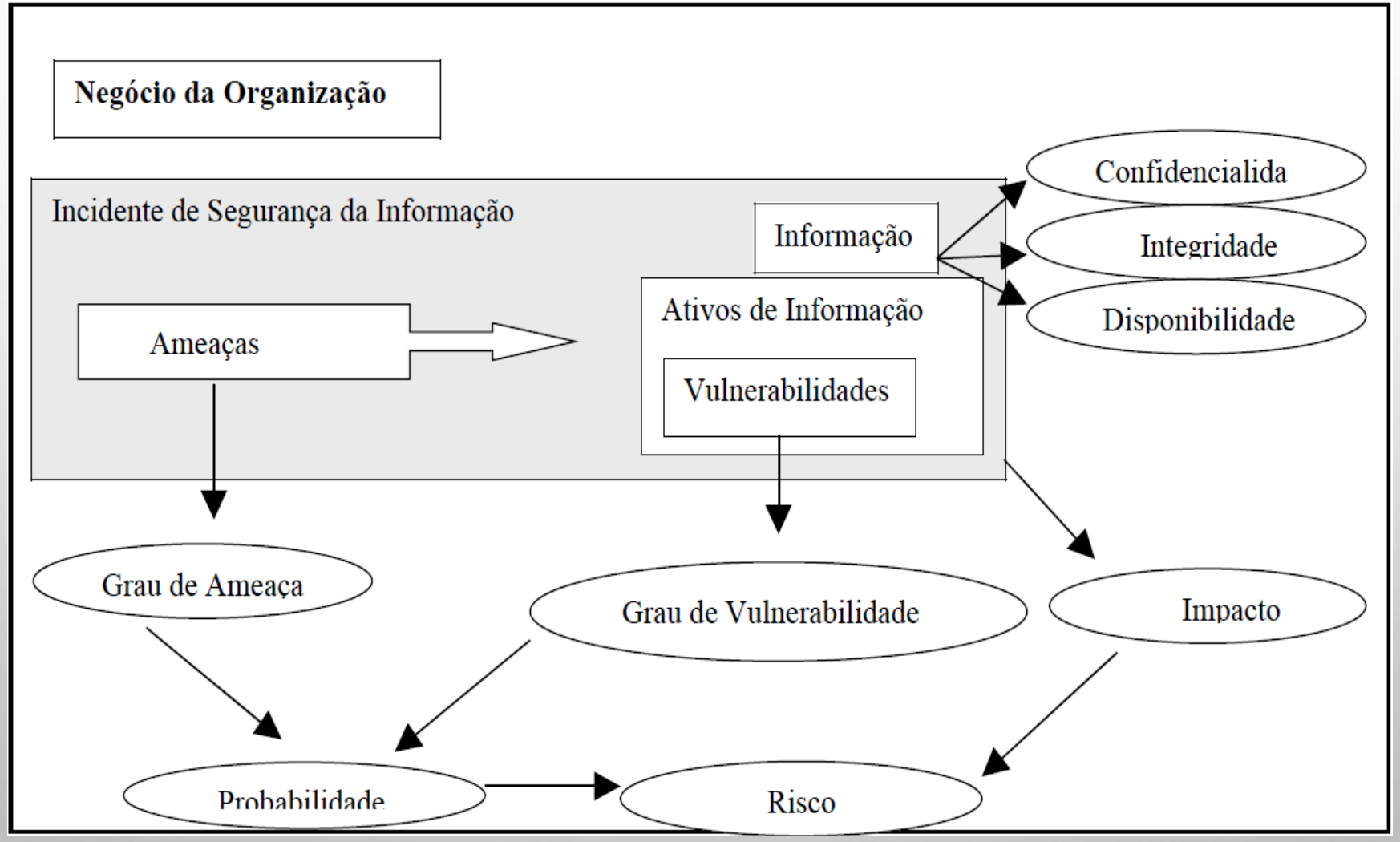
IMPACTO

Resultado da ação bem sucedida de uma ameaça ao explorar as vulnerabilidades de um ativo, atingindo assim um ou mais conceitos da segurança da informação. O impacto se denomina pelos danos/prejuízos causados por um incidente de segurança da informação ocorrido no negócio organização.

O tamanho ou grau de um impacto no negócio da organização depende do grau da relevância dos ativos de informação para os processos da organização, ou seja, quanto maior for a relevância do ativo para a organização, maior será o impacto de um incidente de segurança da informação caso ele venha acontecer.

É preciso definir um grau de impacto para cada incidente de segurança da informação que possa vir ocorrer. Este grau de impacto será de extrema importância para o cálculo do risco, que veremos mais à frente.

INTRODUÇÃO


Negócio da Organização
Incidente de Segurança da Informação
Informação
Confidencialida
Integridade
Disponibilidade
Ativos de Informação
Ameaças
Vulnerabilidades
Grau de Ameaça
Grau de Vulnerabilidade
Impacto
Probabilidade
Risco

ATIVO

- QUALQUER ITEM (FÍSICO OU LÓGICO) QUE REQUER PROTEÇÃO CONTRA PERDA DE INTEGRIDADE, DISPONIBILIDADE OU CONFIDENCIALIDADE.

AMEAÇA (THREAT)

- UMA AMEAÇA É UMA VIOLAÇÃO POTENCIAL DE UM OU MAIS ATIVOS QUE UMA FONTE DE AMEAÇAS PODE CAUSAR AO EXPLORAR COM SUCESSO UMA DETERMINADA VULNERABILIDADE.
- SITUAÇÃO POTENCIAL DE PREJUÍZO OU PERDA.
  - EXEMPLOS:
    - ROUBO.
    - DESTRUIÇÃO DEVIDO A INCÊNDIO.
    - MAL FUNCIONAMENTO DE EQUIPAMENTO.
    - INTRUSOS NO SISTEMA.
    - PERDA DE ARQUIVO.

FONTE DE AMEAÇA

- UMA FONTE DE AMEAÇAS É QUALQUER CIRCUNSTÂNCIA OU EVENTO QUE PODE CAUSAR DANO PARA UM SISTEMA DE INFORMAÇÃO.
- EXEMPLO:
  - EX-FUNCIONÁRIO VINGATIVO.
  - ESPIÃO.
  - INCÊNDIO.
  - FURACÃO.

VULNERABILIDADE

- FRAGILIDADE QUE PODE SER EXPLORADA POR UMA OU MAIS FONTES DE AMEAÇAS.
- A VULNERABILIDADE PODE AMPLIAR O EFEITO DE UMA AMEAÇA.
- EXEMPLO:
  - LOGIN DE EX-FUNCIONÁRIO ATIVO.
  - PROTEÇÃO CONTRA INCÊNDIO INADEQUADO.
  - TELAS DE FUNCIONÁRIOS COM FÁCIL ACESSO PARA VISITANTES.

FONTE DE AMEAÇAS E VULNERABILIDADES

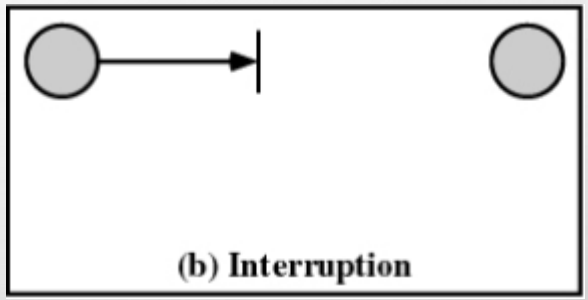
- AS FONTES DE AMEAÇAS REQUEREM A EXISTÊNCIA DE VULNERABILIDADES.
- UMA FONTE DE AMEAÇA É INÓCUA SE NÃO EXISTIR UMA VULNERABILIDADE A SER EXPLORADA.

ATAQUE

- UM ATAQUE É A TENTATIVA DE CAUSAR UMA AMEAÇA ATRAVÉS DA EXPLORAÇÃO DE UMA VULNERABILIDADE POR UMA FONTE DE AMEAÇA.

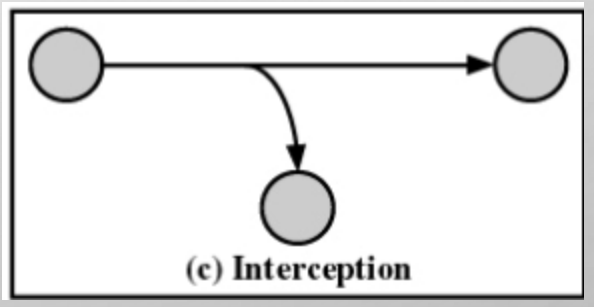
TIPOS DE ATAQUES

- INTERRUPÇÃO
  - UM ATIVO É DESTRUIDO OU FICA NÃO DISPONÍVEL.
  - EXEMPLOS:
    - ATAQUES DOS (DENIAL OF SERVICE).
    - DESTRUIÇÃO DE HARDWARE
    - CORTE DE LINHAS DE COMUNICAÇÃO.
    - CORTE NO FORNECIMENTO DE ENERGIA.
    - DESABILITAÇÃO DO SISTEMA DE ARQUIVOS.



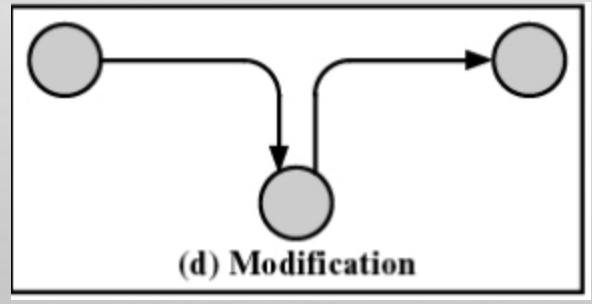
TIPOS DE ATAQUES

- INTERCEPTAÇÃO
  - UMA ELEMENTO NÃO AUTORIZADO GANHA ACESSO A UM ATIVO.
  - EXEMPLOS:
    - ATAQUE SOBRE A CONFIDENCIALIDADE
    - ESCUTA DE CABOS DE COMUNICAÇÃO
    - CÓPIAS ILÍCITAS DE ARQUIVOS
    - MONITORAMENTO DE TRÁFEGO



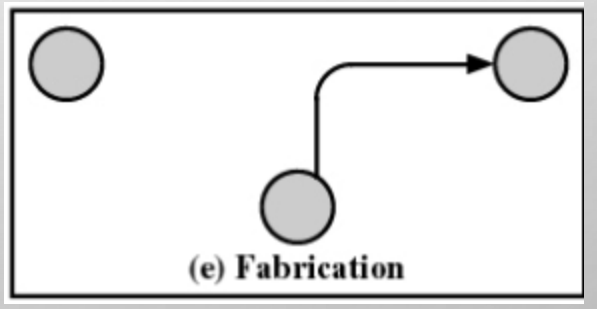
TIPOS DE ATAQUES

- MODIFICAÇÃO
  - UM USUÁRIO NÃO AUTORIZADO MODIFICA UM ATIVO.
  - ATAQUE SOBRE A INTEGRIDADE
    - MODIFICAR CONTEÚDO DE ARQUIVO.
    - ALTERAR PROGRAMAS.
    - MODIFICAR CONTEÚDO DE MENSAGENS NA REDE.



TIPOS DE ATAQUES

- FABRICAÇÃO
  - UM ELEMENTO NÃO AUTORIZADO INSERE OBJETOS FALSOS NO SISTEMA.
  - ATAQUE SOBRE A AUTENTICIDADE OU NÃO REPUDIAÇÃO.
    - INSERÇÃO DE MENSAGENS ESPÚRIAS.
    - INSERÇÃO DE REGISTROS NÃO EXISTENTES EM ARQUIVOS.
    - ALTERAÇÃO DO CONTEÚDO DE PÁGINAS WEB.



RISCO

- RISCO É A EXPECTATIVA DO EFEITO DE UMA AMEAÇA.
- COMPOSTO POR
  - PROBABILIDADE DA AMEAÇA.
  - EXTENSÃO DO DANO CAUSADO.
- RISCO= AMEAÇA X DANO

GERÊNCIA DE RISCOS

- IDENTIFICAR AMEAÇAS, FONTES DE AMEAÇAS E VULNERABILIDADES.
- IDENTIFICAR PROBABILIDADES DE OCORRÊNCIAS.
- IDENTIFICAR POSSÍVEIS DANOS.
- AÇÕES:
  - ELIMINAR RISCOS.
  - MINIMIZAR.
  - ACEITAR.

FUNCIONALIDADE E GARANTIA

- NA AVALIAÇÃO DE SEGURANÇA DE SISTEMAS, DOIS ASPECTOS NECESSITAM SER CONSIDERADOS:
  - FUNCIONALIDADE: QUAIS SÃO AS FUNÇÕES DE SEGURANÇA PROVIDAS?
  - GARANTIA: QUAL É A GARANTIA DE QUE AS FUNÇÕES FUNCIONAM CONFORME O DECLARADO?
- ESTES DOIS ASPECTOS DEVEM SER CONSIDERADOS NO PROCESSO DE AVALIAÇÃO.

GARANTIA E COMPLEXIDADE

- O TRABALHO NECESSÁRIO PARA FAZER A AVALIAÇÃO DE SEGURANÇA É PROPORCIONAL A COMPLEXIDADE DO SISTEMA.
- ASSIM SE É DESEJÁVEL UM CERTO NÍVEL DE GARANTIA, É NECESSÁRIO MINIMIZAR A COMPLEXIDADE.

3 PERSPECTIVAS PARA SEGURANÇA

- GERÊNCIA
  - ABORDA QUESTÕES RELATIVO A GESTÃO DE SEGURANÇA NO CICLO DE VIDA DO SISTEMA.
- OPERAÇÕES
  - ABORDA QUESTÕES DE SEGURANÇA NA INSTALAÇÃO E OPERAÇÃO DO SISTEMA.
- TECNOLOGIA
  - ABORDA COMPONENTES QUE OFERECEM SERVIÇOS DE SEGURANÇA. POR EXEMPLO, SERVIÇO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE USUÁRIOS.

REQUISITOS DE SEGURANÇA E OS NEGÓCIOS

- CADA NEGÓCIO APRESENTA O SEU CONJUNTO DE REQUISITOS DE SEGURANÇA PARTICULAR.
- UMA VULNERABILIDADE COMUM É PROJETAR A SEGURANÇA ENDEREÇANDO REQUISITOS ERRADOS.

REQUISITOS DE SEGURANÇA EM UM BANCO

- AS PRINCIPAIS OPERAÇÕES DE UM BANCO ESTÃO RELACIONADAS AO GERENCIAMENTO DE CONTAS DE CLIENTES.
  - TRANSAÇÕES DIÁRIAS DE CRÉDITOS E DÉBITOS.
  - A PRINCIPAL AMEAÇA É O STAFF INTERNO.
  - A PRINCIPAL DEFESA SÃO OS PROCEDIMENTOS DE CONTROLE (SECULAR).
  - SISTEMAS DE AUDITORIA.
  - SISTEMAS DE MONITORAMENTO DE DISCREPÂNCIAS.
  - ATENDIMENTO A LEGISLAÇÃO.

CONT.

- INTERFACES COM SISTEMAS DE MENSAGENS
  - TRANSFERÊNCIAS PARA OUTRAS CONTAS.
  - TRANSFERÊNCIAS PARA INVESTIMENTOS.
  - EMISSÃO DE CARTAS DE CRÉDITO.
- INTERFACES COM O PÚBLICO
  - ATM
  - WEB
- PROTEÇÃO PARA A AGÊNCIA, ATMS E SALA COFRE
  - SISTEMA DE ALARMES LIGADO A UMA CENTRAL.

REQUISITOS DE SEGURANÇA EM UMA ORGANIZAÇÃO MILITAR

- PROTEÇÃO ELETRÔNICA CONTRA INTERFERÊNCIAS.
- SISTEMA DE COMUNICAÇÃO SEGURO E PROTEGIDO CONTRA LOCALIZAÇÃO.
- PROTEÇÃO DO SISTEMA DE LOGÍSTICA.
- POLÍTICAS PARA FLUXO DE INFORMAÇÕES.
- PROTEÇÃO DO SISTEMA DE COMANDO E CONTROLE.

REQUISITOS DE SEGURANÇA EM UM HOSPITAL

- SEGURANÇA QUANTO A PRECISÃO DAS INFORMAÇÕES DISPONIBILIZADAS.
- PRIVACIDADE DE PACIENTES.
- ANONIMIZAÇÃO DE DADOS DE PACIENTES PARA ENSINO E PESQUISA.
- DISPONIBILIDADE DOS SISTEMAS DE INFORMAÇÃO É UM REQUISITO CRÍTICO.

REQUISITOS DE SEGURANÇA EM RESIDÊNCIAS

- SEGURANÇA DE SISTEMAS DE VIGILÂNCIA DE RESIDÊNCIAS, VEÍCULOS E PESSOAS.
- SEGURANÇA DE SISTEMAS DE COMUNICAÇÃO.
- SEGURANÇA PARA MEDIDORES DE GÁS, LUZ, ÁGUA, ETC.
- SEGURANÇA PARA ACESSO REMOTO A DISPOSITIVOS DOMÉSTICOS.
- SISTEMAS DOMÉSTICOS PODEM SER A PORTA DE ENTRADA PARA SISTEMAS EMPRESARIAIS.

ANÁLISE DE IMPACTO AO NEGÓCIO (BIA)

É feita buscando identificar os processos críticos que apoiam o negócio da organização, e qual impacto para o negócio caso as ameaças mapeadas venham a se concretizar.

Calculo do Impacto

$$\textbf{Impacto} = \frac{(\text{Relevância do Processo} + \text{Relevância do Ativo})}{2}$$

Relevância do Processo: Importância do processo ao negócio.

Relevância do Ativo: Importância do ativo no processo de negócio.

ANÁLISE DE RISCOS (AR)

- É realizada para identificar os riscos aos quais estão submetidos os ativos, ou seja, para saber qual é a probabilidade de que as ameaças se concretizem e o impacto que elas causarão ao negócio.

- A análise de risco possibilita identificar o grau de proteção que os ativos de informação precisam, podendo assim, não só proporcionar o grau adequado de proteção a esse ativo, mas principalmente utilizar de forma inteligente os recursos da organização.

SI – ANÁLISE DE RISCOS (AR)

Calculo de Risco de um Incidente a um Ativo?

$$\textbf{Risco} = \frac{(\text{Probabilidade} + \text{Impacto} + \text{Índice ocorrências anteriores})}{3}$$

Onde:

$$\textbf{Probabilidade} = \frac{(\text{Grau de Ameaça} + \text{Grau de Vulnerabilidade})}{2}$$

Índice de Ocorrências = (Total de dias no ano* em que houve incidentes)

* Ano = 365 dias SEMPRE.

SI - CONCLUSÃO

- A Segurança da Informação é um processo que envolve todas as áreas de negócio de uma organização e deve ser entendida como mais uma disciplina orientada a atingir a missão estabelecida.