INSTITUTO FEDERAL
PIAUÍ
Campus Parnaíba

Princípios da Segurança

Prof. Msc Denival A. dos Santos

Ativos

- Definição: é tudo aquilo que possui valor para uma organização.
- Valor: quantificação de perda de determinado ativo quando esse tem sua confidencialidade, integridade ou disponibilidade afetas.
- Vulnerabilidade: falha no ambiente que ameaça algum ativo.
- Ameaça: possibilidade de exploração de uma vulnerabilidade.
- Impacto: Resultado da concretização de uma ameaça contra a vulnerabilidade de um ativo.
- Classificação:
  - Tangíveis: Aplicativos, equipamentos, usuários, etc.
  - Intangíveis: Imagem de uma empresa, marca de um produto, confiabilidade de um órgão, etc..
  - Lógicos: Dados armazenados em um servidor.
  - Físicos: Estações de trabalho, sistema de ar-condicionado, cofre.
  - Humanos: Empregados, prestadores de serviços.

Ativos

Tudo que manipula informação, inclusive ela mesma.

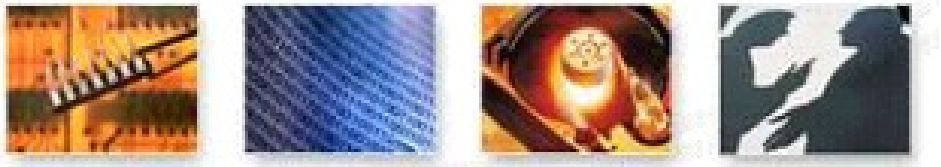
Ativos são os elementos que sustentam a operação do seu negócio e estes sempre trarão consigo

VULNERABILIDADES

que, por sua vez, submetem os ativos a

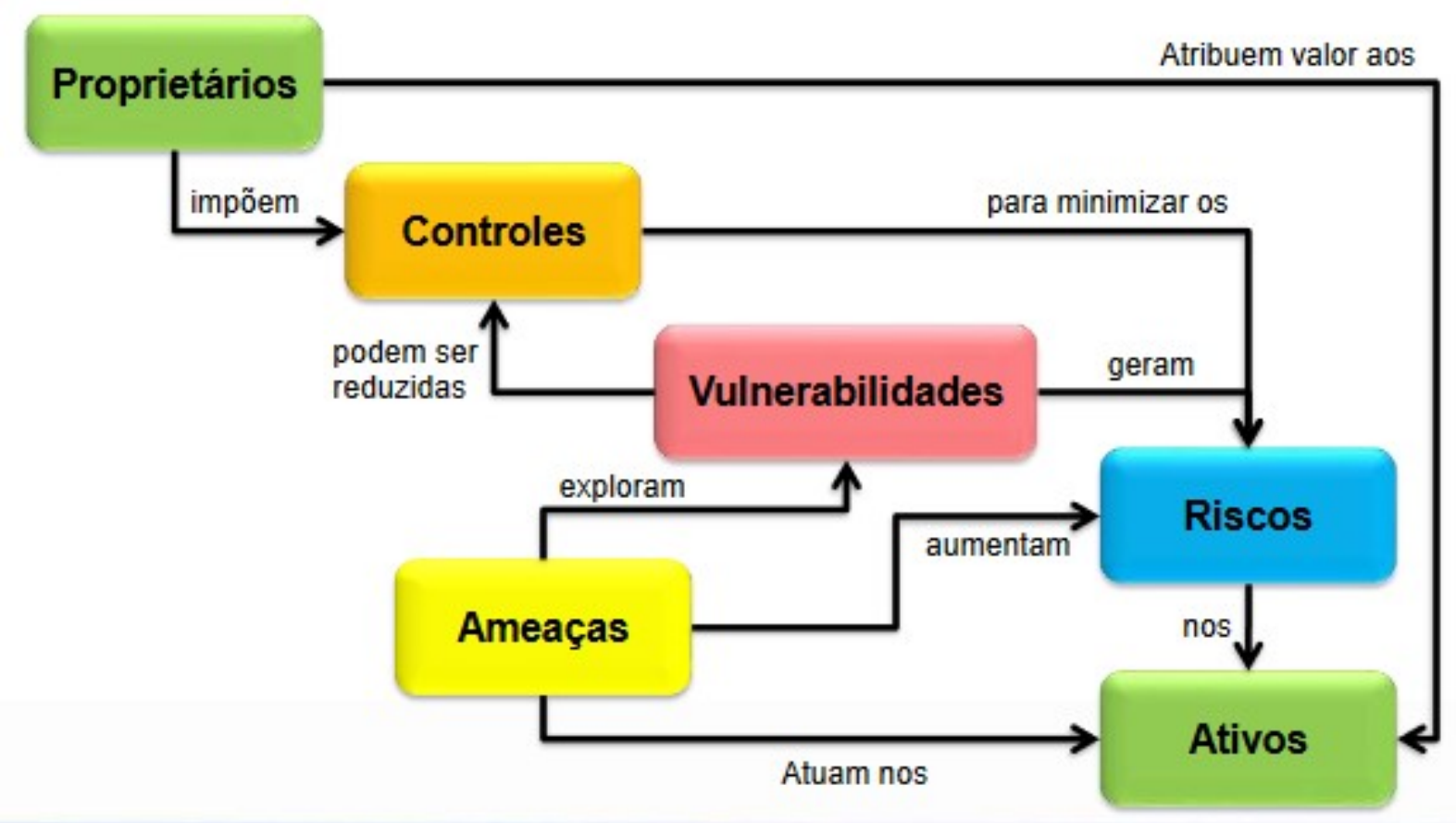
AMEAÇAS

Exemplos de Ativos:



HARDWARE SOFTWARE BACKUP HUMANO

Ativos


Proprietários
Atribuem valor aos
impõem
Controles
para minimizar os
podem ser reduzidas
Vulnerabilidades
geram
exploram
Riscos
aumentam
Ameaças
nos
Ativos
Atuam nos

Classificação dos Ativos

- São três os elementos que compõem o que chamamos de ativos:
  - As informações;
  - As pessoas que as utilizam;
  - Os equipamentos e sistemas que oferecem suporte a elas;
    - Software;
    - Hardware;
    - Organização.

Exemplo - Backup

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?

Exemplo - Humano

Exemplo de Ativo:

A **desatualização tecnológica** é uma das vulnerabilidades com maior numero de ocorrências dentro das organizações..

Exemplo - Software

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.

Exemplo - Hardware

Hardware

- Esses ativos representam toda a infraestrutura tecnológica que oferece suporte à informação durante seu uso, trânsito, processamento e armazenamento. Faz parte desse grupo qualquer equipamento no qual se armazene, processe ou transmita as informações da empresa:
  - as estações de trabalho
  - os servidores
  - os computadores portáteis
  - os mainframes
  - as mídias de armazenamento

Possíveis vulnerabilidades

Infra-estrutura elétrica sujeita a falhas que danifiquem os equipamentos, centros de computação sujeitos a inundações, computadores portáteis sem vigilância em locais públicos.

Organizações

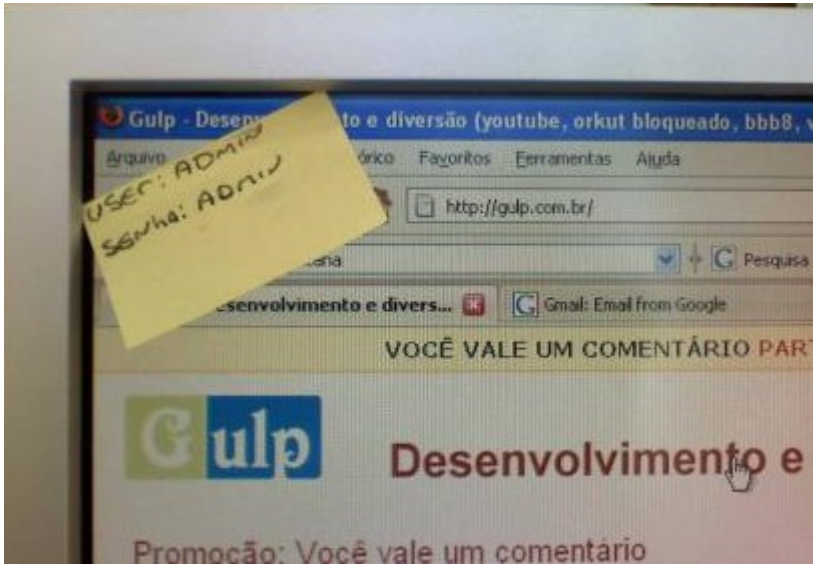
- Neste grupo, estão incluídos os aspectos que compõem a estrutura física e organizacional das empresas. Refere-se à organização lógica e física do pessoal dentro da empresa em questão.
- Em relação ao ambiente físico, entre outros, são considerados:
  - salas e armários onde estão localizados os documentos, fototeca, sala de servidores de arquivos;

Possíveis vulnerabilidades

- ❒ Localização insegura de documentos, equipamentos ou pessoas.
- ❒ Estrutura organizacional que não permita mudanças em termos de segurança.
- ❒ Ausência de equipe dedicada de segurança.

Usuários

- O usuários refere-se aos indivíduos que utilizam a estrutura tecnológica e de comunicação da empresa e que lidam com a informação.
- O enfoque da segurança nos usuários está voltado para a formação do hábito da segurança em todos os funcionários de uma empresa para tomar decisões e empreender ações, desde a alta direção até os usuários finais da informação.



Possíveis vulnerabilidades

- ❒ Desconhecimento dos métodos de escolha de senhas fortes.
- ❒ Resistência de funcionários a adotar práticas de segurança.
- ❒ Descuido por parte dos usuários na manipulação da informação.

Ameaças

- Ameaças sempre existirão e estão relacionadas a causas que representam riscos, as quais podem ser:
  - causas naturais ou não naturais;
  - causas internas ou externas;
- As ameaças são constantes e podem ocorrer a qualquer momento. Elas podem se dividir em três grandes grupos:
  - **Ameaças naturais** - condições da natureza e a intempérie que poderão provocar danos nos ativos, tais como fogo, inundação, terremotos.
  - **Intencionais** - são ameaças deliberadas, fraudes, vandalismo, sabotagens, espionagem, invasões e furtos de informações, entre outros.
  - **Involuntárias** - são ameaças resultantes de ações inconscientes de usuários, por vírus eletrônicos, muitas vezes causados pela falta de conhecimento no uso dos ativos, tais como erros e acidentes.

Princípios básicos da Segurança da informação

- Proteger os ativos significa adotar medidas para evitar a concretização de ameaças que podem afetar a informação: Corrompendo-a, tendo acesso a ela de forma indevida, ou mesmo, eliminando-a ou furtando-a.
- A segurança da informação busca proteger os ativos de uma empresa ou indivíduo com base na preservação de três princípios básicos, conforme (ISO/IEC 17999, 2003; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002), são:
  - Integridade
  - Confidencialidade
  - Disponibilidade
- Outros autores (Dias, 2000; Wadlow, 2000; Shirey, 2000; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002; Sêmola, 2003; Sandhu e Samarati, 1994) defendem que para uma informação ser considera segura, o sistema que o administra ainda deve respeitar:
  - Autenticidade
  - Não repúdio
  - Legalidade
  - Privacidade

Princípios da integridade

- Conceito: garantia de que o conteúdo da mensagem não foi alterado ou violado indevidamente ou não autorizada.
- Garantia: o receptor deverá ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição pelo emissor para uma determinada finalidade.
- Há perda de integridade quando a informação é alterada indevidamente ou quando não se pode garantir que a informação é a mais atualizada.
- Exemplo de quebra de integridade:
  - Falsificação de documentos.
  - Alteração de registro no BD.

Principio da confidencialidade

- O princípio da confidencialidade da informação tem como objetivo garantir que apenas a pessoa correta tenha acesso à informação;
- Ter confidencialidade na comunicação é ter a segurança de que o que foi dito a alguém ou escrito em algum lugar só será escutado ou lido por quem tiver autorização para tal;
- Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá ser guardada com segurança, e não divulgada para pessoas não autorizadas
- Exemplo:

  Pensemos no caso de um cartão de crédito. O número do cartão só poderá ser conhecido por seu proprietário e pela loja onde é usado. Se esse número for descoberto por alguém mal-intencionado, como nos casos noticiados sobre crimes da Internet, o prejuízo causado pela perda de confidencialidade poderá ser muito elevado;

Princípios da Disponibilidade

- A informação deve chegar apenas aos destinatários ou usuários adequados e de forma íntegra, devemos fazer com que esteja disponível no momento oportuno;
- Para que uma informação possa ser utilizada, ela deve estar disponível;
- A disponibilidade da informação permite que:
  - Seja utilizada quando necessário;
  - Esteja ao alcance de seus usuários e destinatários;
  - Possa ser acessada no momento em que for necessário utilizá-la;
- Exemplo:
  - Durante uma reunião de altos executivos da empresa, os serviços de banco de dados falham, o que impede que se tome uma decisão central em termos de negócios.