Princípios básicos de segurança da informação.

Auditoria e Segurança de SI

UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

Prof. Roberto Cabral

rbcabral@ufc.br

Universidade Federal do Ceará

1º semestre/2023

Ementa

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).
- Softwares maliciosos.

Ementa

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).
- Softwares maliciosos.
- O conceito e os objetivos da auditoria de sistemas de informação.

Ementa

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).
- Softwares maliciosos.
- O conceito e os objetivos da auditoria de sistemas de informação.
- Técnicas de auditoria. Softwares de auditoria.

Ementa

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).
- Softwares maliciosos.
- O conceito e os objetivos da auditoria de sistemas de informação.
- Técnicas de auditoria. Softwares de auditoria.
- Técnicas de software seguro.

Ementa

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Propriedades da segurança da informação: confidencialidade, integridade, autenticidade, disponibilidade.
- Tipos de ataque.
- Noções de criptografia.
- Funções de resumo.
- Assinaturas digitais.
- Certificados digitais.
- Infraestrutura de chaves públicas (ICP-Brasil).
- Softwares maliciosos.
- O conceito e os objetivos da auditoria de sistemas de informação.
- Técnicas de auditoria. Softwares de auditoria.
- Técnicas de software seguro.
- Norma NBR27002.

Objetivos

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Apresentar os conceitos de segurança da informação e suas aplicações.
- Identificar ameaças e vulnerabilidades em ativos de informação.
- Despertar os alunos para a necessidade de proteção de dados sensíveis e para a habilidade de reconhecimento de identidade em um ambiente inseguro, além de apresentá-los às técnicas criptográficas mais utilizadas.

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:
  - Seminário

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:
  - Seminário
  - Exercícios de fixação.

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:
  - Seminário
  - Exercícios de fixação.
  - Atividade Prática.

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:

Avaliações

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;

Avaliações

- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;
  - Dois seminários, s_1 e s_2;

Avaliações

- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;
  - Dois seminários, s_1 e s_2;
  - x Labs, l_i para $0 < i \leq x$.

Avaliações

- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;
  - Dois seminários, s_1 e s_2;
  - x Labs, l_i para $0 < i \leq x$.
- Composição da Nota:

Avaliações

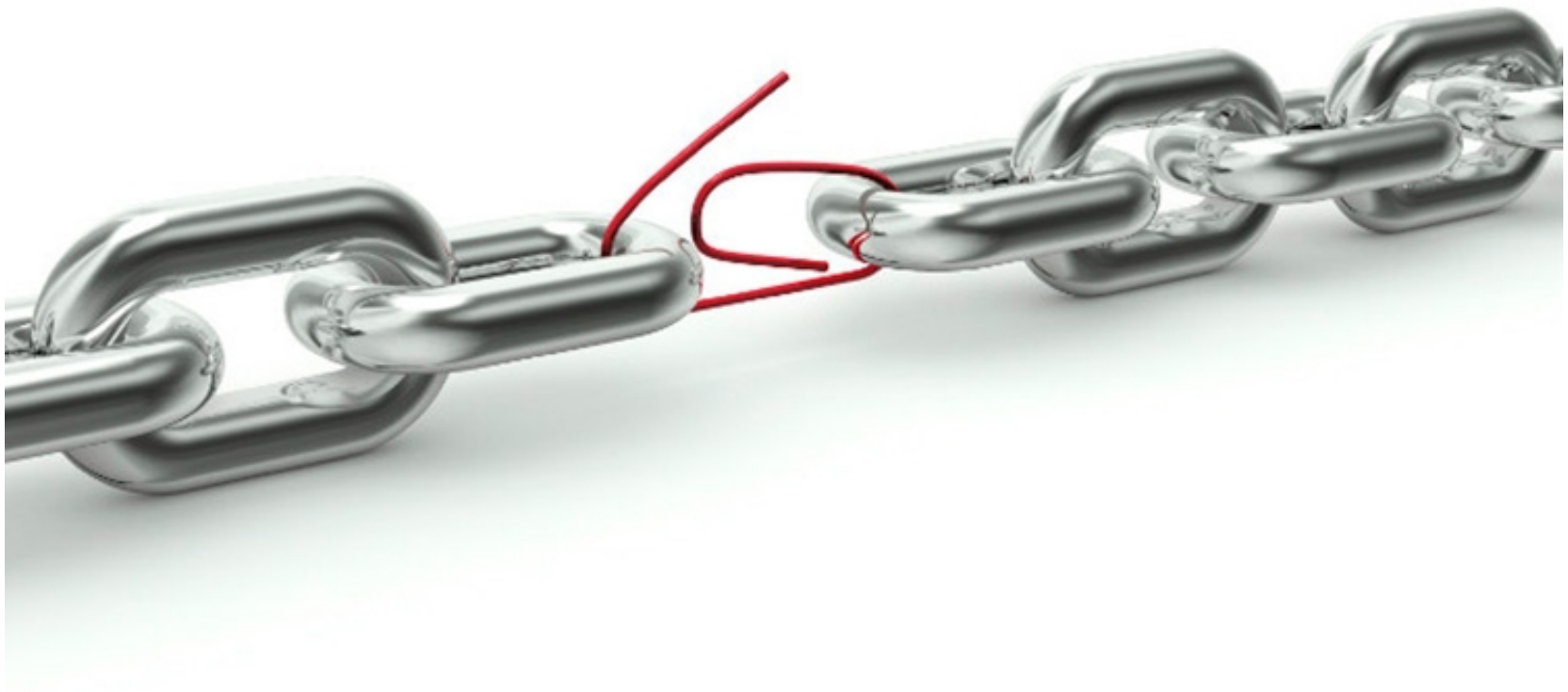
- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;
  - Dois seminários, s_1 e s_2;
  - x Labs, l_i para $0 < i \leq x$.
- Composição da Nota:
  - Seja L a média dos labs, temos:

Avaliações

- Avaliações:
  - Duas avaliações parciais, p_1 e p_2;
  - Dois seminários, s_1 e s_2;
  - x Labs, l_i para $0 < i \leq x$.
- Composição da Nota:
  - Seja L a média dos labs, temos:
    - $\texttt{Média} = (p_1 + p_2 + s_1 + s_2 + L)/5$.

Dúvidas?

Quão Seguro é um Sistema de Informação?



Conceitos chaves da Segurança da Informação

Acesso

A capacidade de um sujeito ou objeto de usar, manipular, modificar ou afetar outro sujeito ou objeto.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Acesso

A capacidade de um sujeito ou objeto de usar, manipular, modificar ou afetar outro sujeito ou objeto.

Ativo

O recurso organizacional que está sendo protegido.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Acesso

A capacidade de um sujeito ou objeto de usar, manipular, modificar ou afetar outro sujeito ou objeto.

Ativo

O recurso organizacional que está sendo protegido.

Ataque

Um ato intencional ou não intencional que pode danificar ou comprometer informações e os sistemas que as suportam. Os ataques podem ser ativos ou passivos, intencionais ou não intencionais, diretos ou indiretos.

Conceitos chaves da Segurança da Informação

Controle, proteção ou contramedida

Mecanismos, políticas ou procedimentos de segurança que podem combater com sucesso ataques, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização.

Conceitos chaves da Segurança da Informação

Controle, proteção ou contramedida

Mecanismos, políticas ou procedimentos de segurança que podem combater com sucesso ataques, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização.

Vulnerabilidade

Uma fraqueza potencial em um ativo ou em seu(s) sistema(s) de controle defensivo.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Controle, proteção ou contramedida

Mecanismos, políticas ou procedimentos de segurança que podem combater com sucesso ataques, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização.

Vulnerabilidade

Uma fraqueza potencial em um ativo ou em seu(s) sistema(s) de controle defensivo.

Exposição

Uma condição ou estado de exposição; na segurança da informação, a exposição existe quando uma vulnerabilidade é conhecida por um invasor.

Conceitos chaves da Segurança da Informação

Perda

Uma única instância de um ativo de informação que sofre danos ou destruição, modificação ou divulgação não intencional ou não autorizada, ou negação de uso.

Conceitos chaves da Segurança da Informação

Perda

Uma única instância de um ativo de informação que sofre danos ou destruição, modificação ou divulgação não intencional ou não autorizada, ou negação de uso.

Perfil de proteção ou postura de segurança

Todo o conjunto de controles e contramedidas, incluindo política, educação, treinamento e conscientização e tecnologia, que a organização implementa para proteger o ativo.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Perda

Uma única instância de um ativo de informação que sofre danos ou destruição, modificação ou divulgação não intencional ou não autorizada, ou negação de uso.

Perfil de proteção ou postura de segurança

Todo o conjunto de controles e contramedidas, incluindo política, educação, treinamento e conscientização e tecnologia, que a organização implementa para proteger o ativo.

Risco

A probabilidade de uma ocorrência indesejada, como um evento adverso ou perda.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Ameaça

Qualquer evento ou circunstância que tenha o potencial de afetar adversamente as operações e os ativos.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Ameaça

Qualquer evento ou circunstância que tenha o potencial de afetar adversamente as operações e os ativos.

Agente de ameaça

A instância específica ou um componente de uma ameaça.

Conceitos chaves da Segurança da Informação

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Ameaça

Qualquer evento ou circunstância que tenha o potencial de afetar adversamente as operações e os ativos.

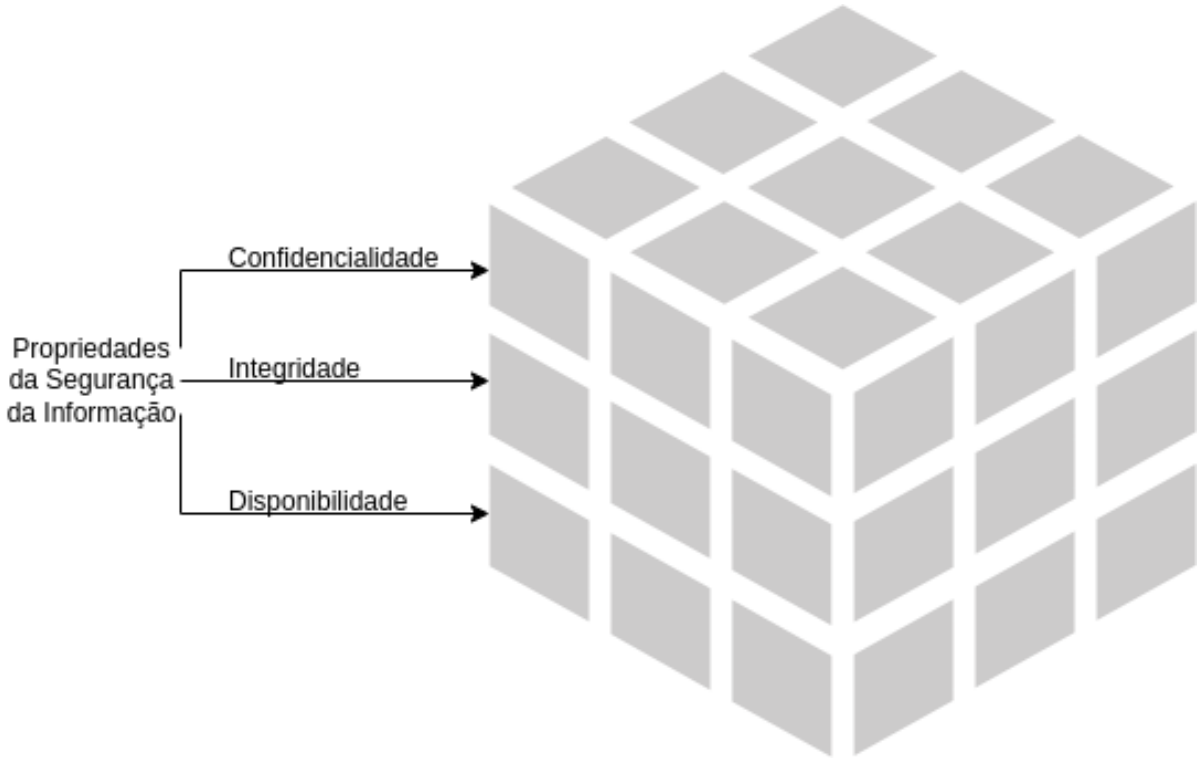
Agente de ameaça

A instância específica ou um componente de uma ameaça.

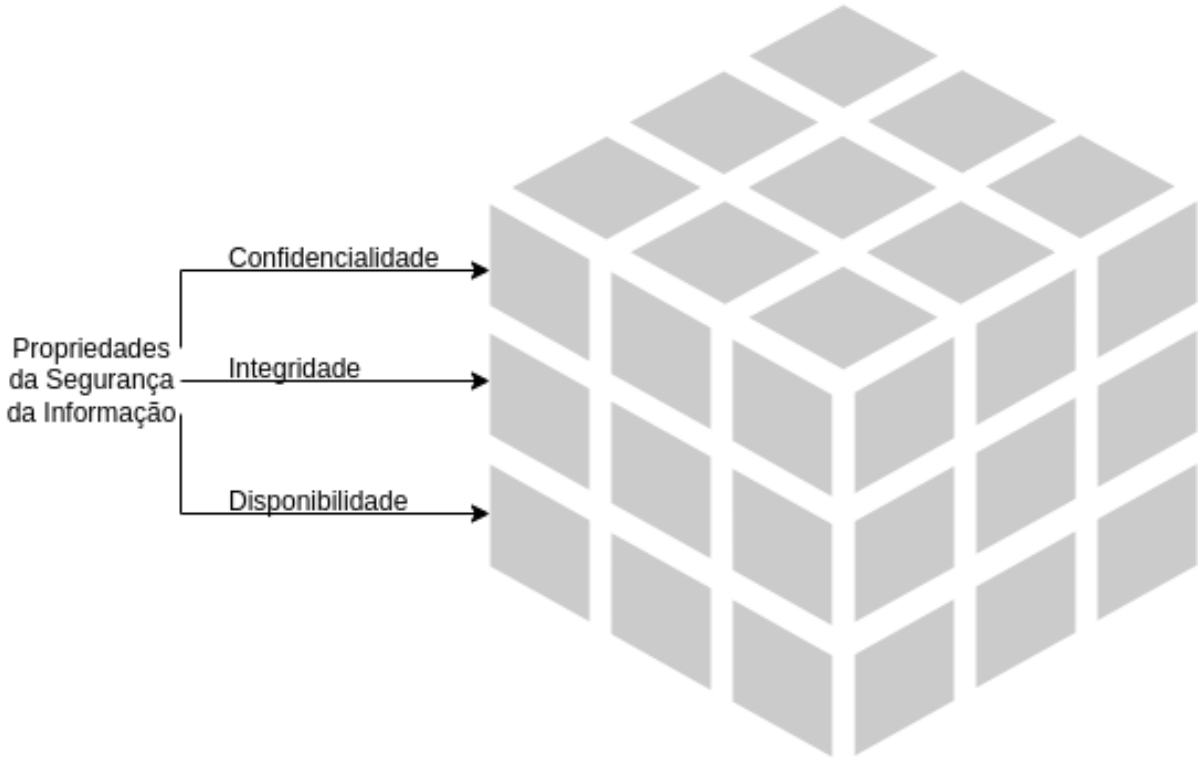
Evento de ameaça

A ocorrência de um evento causado por um agente de ameaça.

Cubo de McCumber



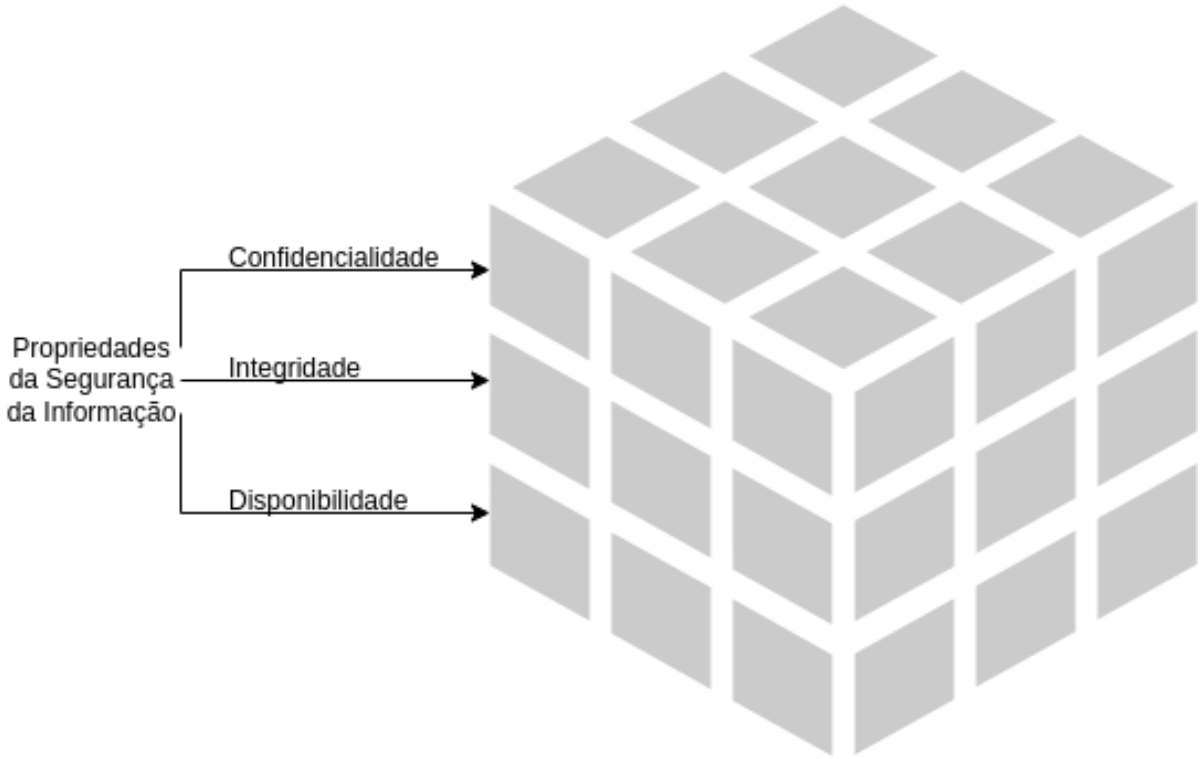
Cubo de McCumber



Confidencialidade

Garantir que as informações confidenciais não sejam divulgadas intencionalmente ou acidentalmente por pessoas não autorizadas.

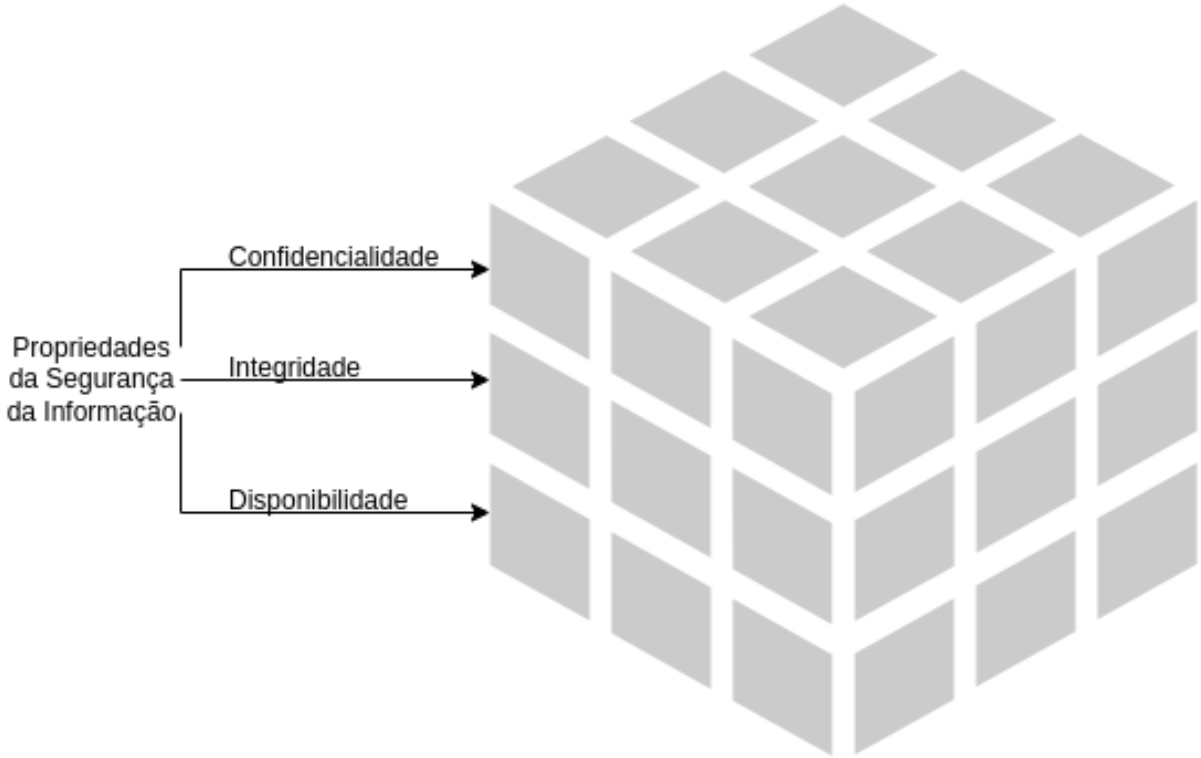
Cubo de McCumber



Integridade

Garantir que as informações não sejam modificadas intencionalmente ou acidentalmente.

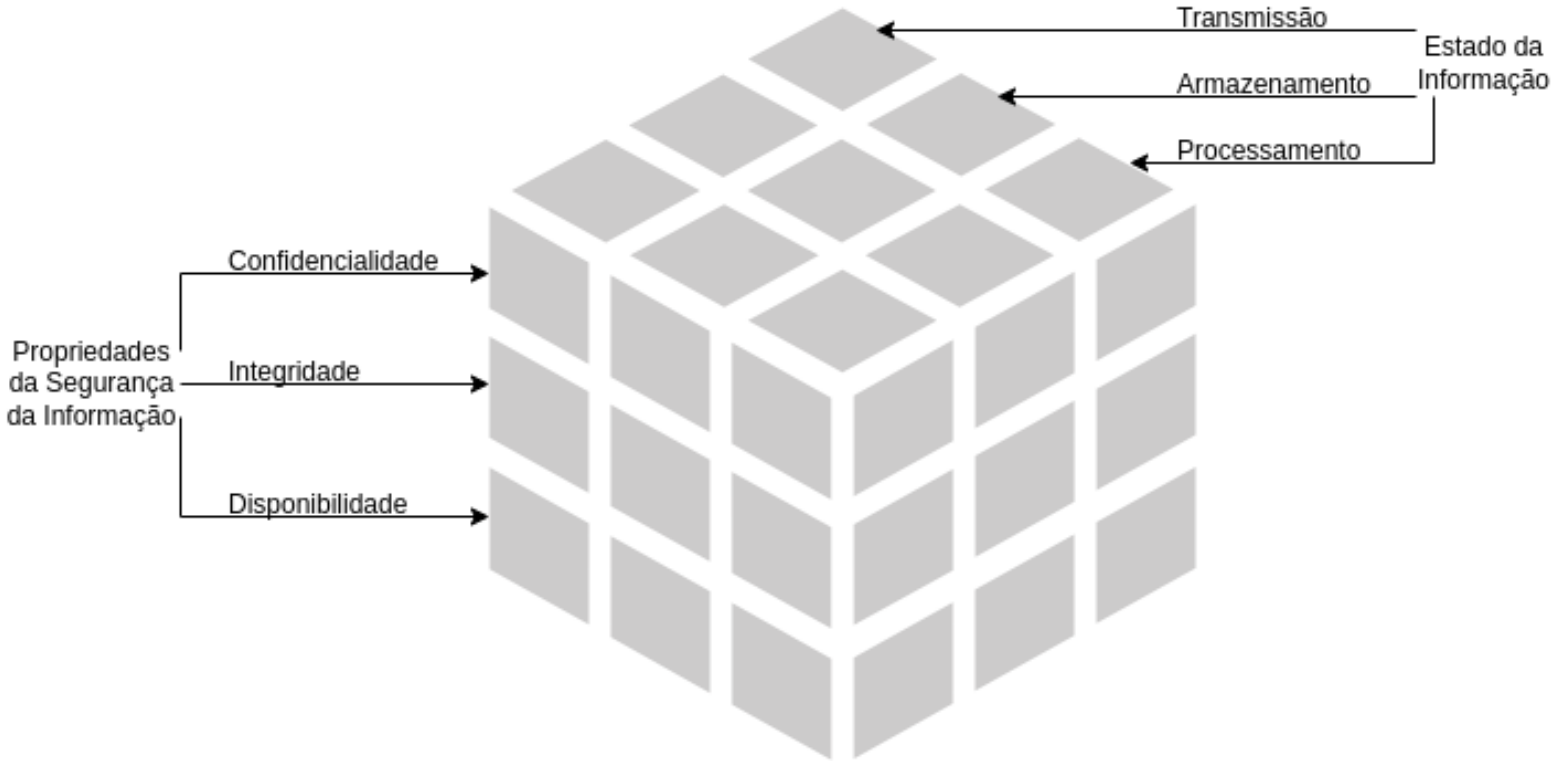
Cubo de McCumber



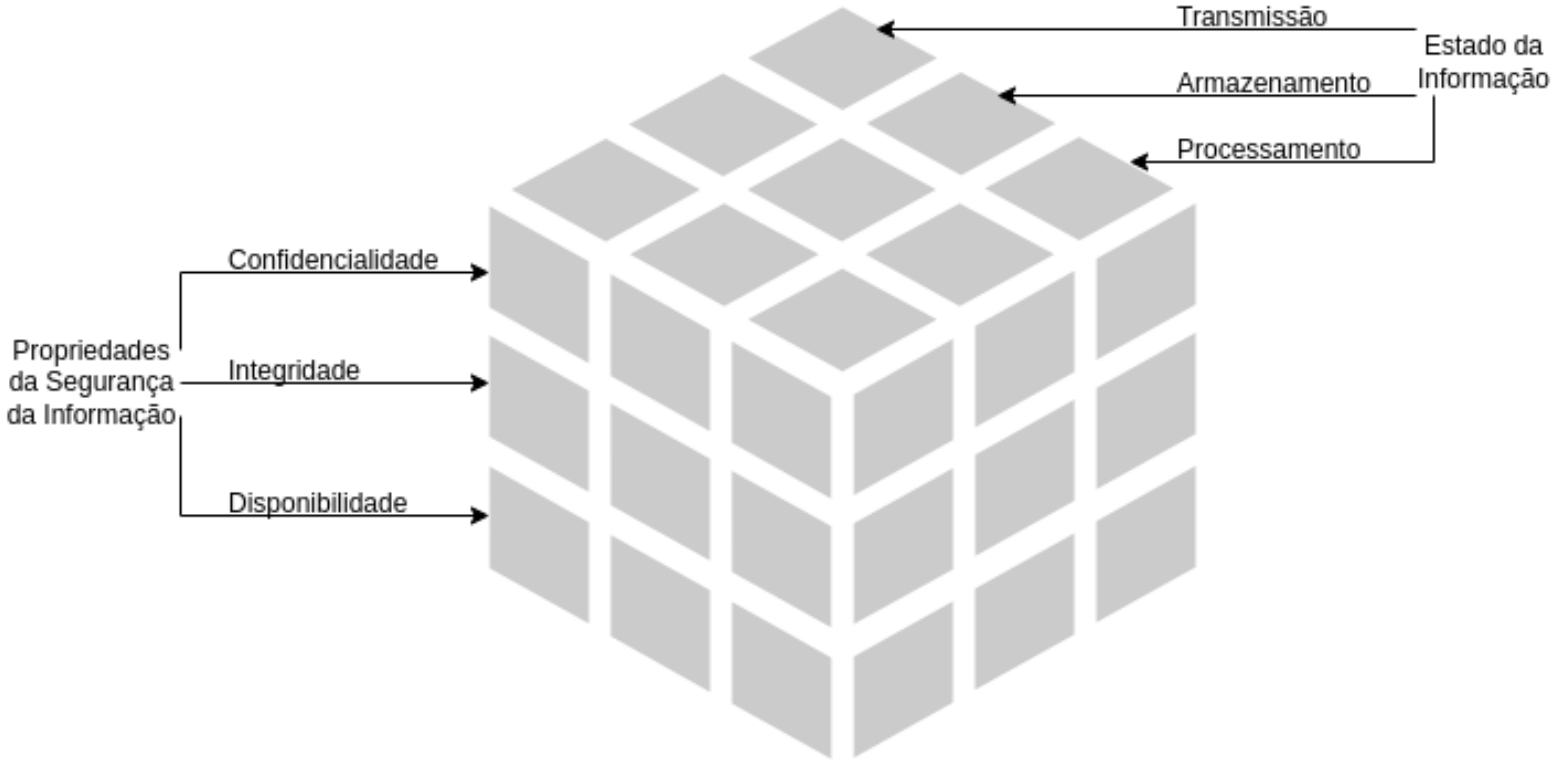
Disponibilidade

Garantir que as pessoas autorizadas tenham acesso seguro e em tempo oportuno às informações e aos sistemas de informação.

Cubo de McCumber



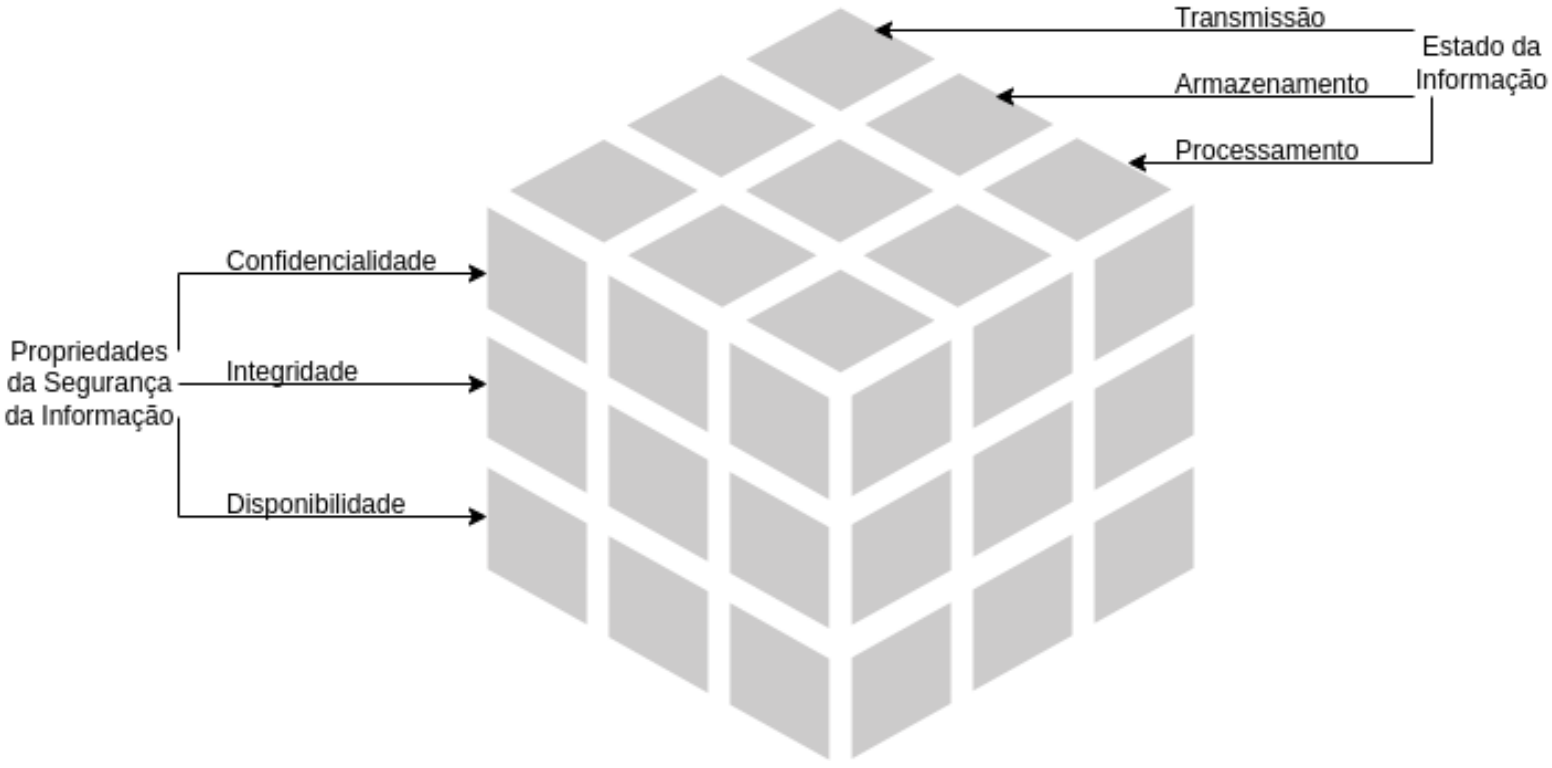
Cubo de McCumber



Transmissão

Transferência de dados entre Sistemas de Informação.

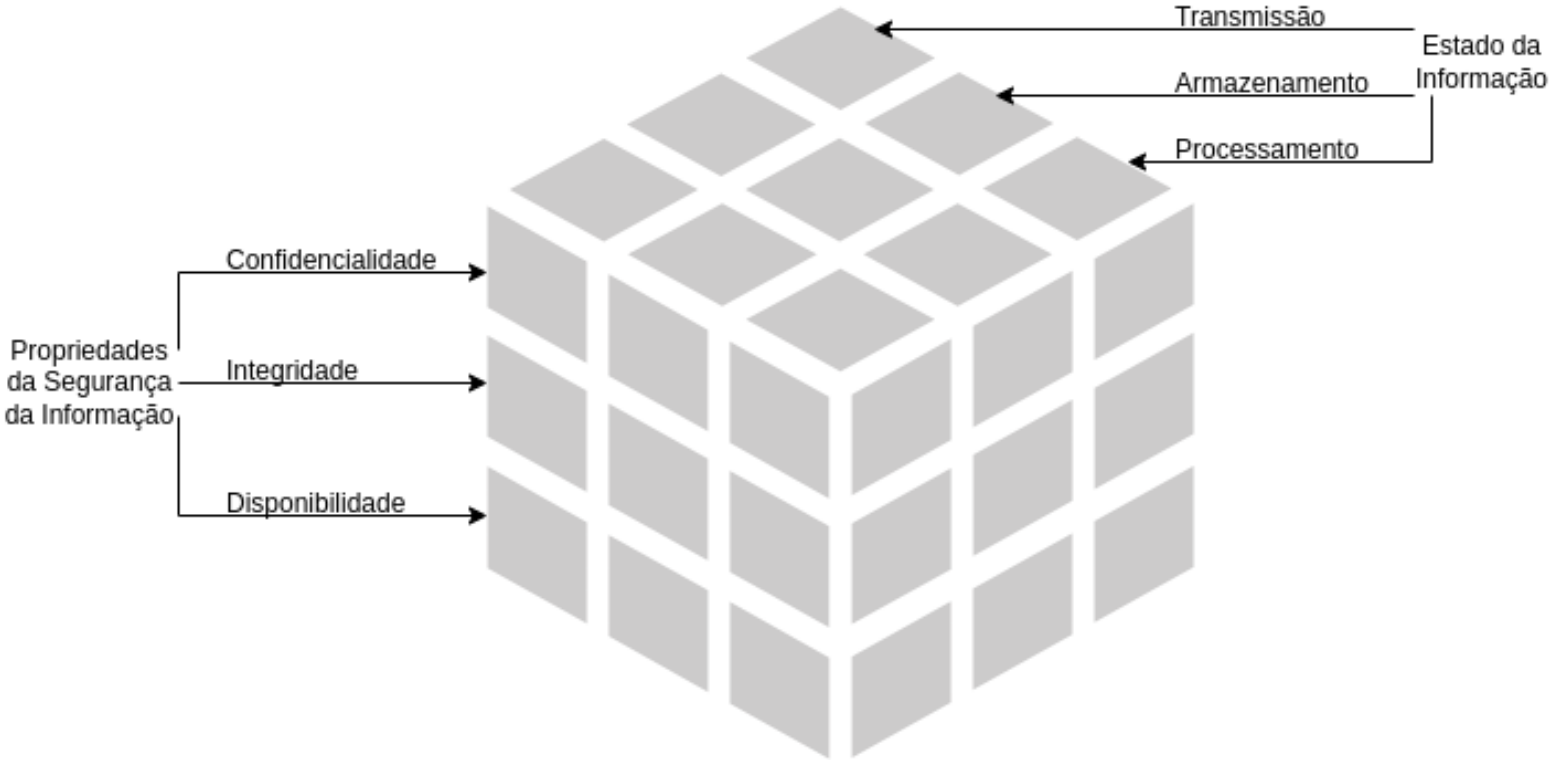
Cubo de McCumber



Armazenamento

Armazenamento local e remoto dos dados (Ativos e Inativos).

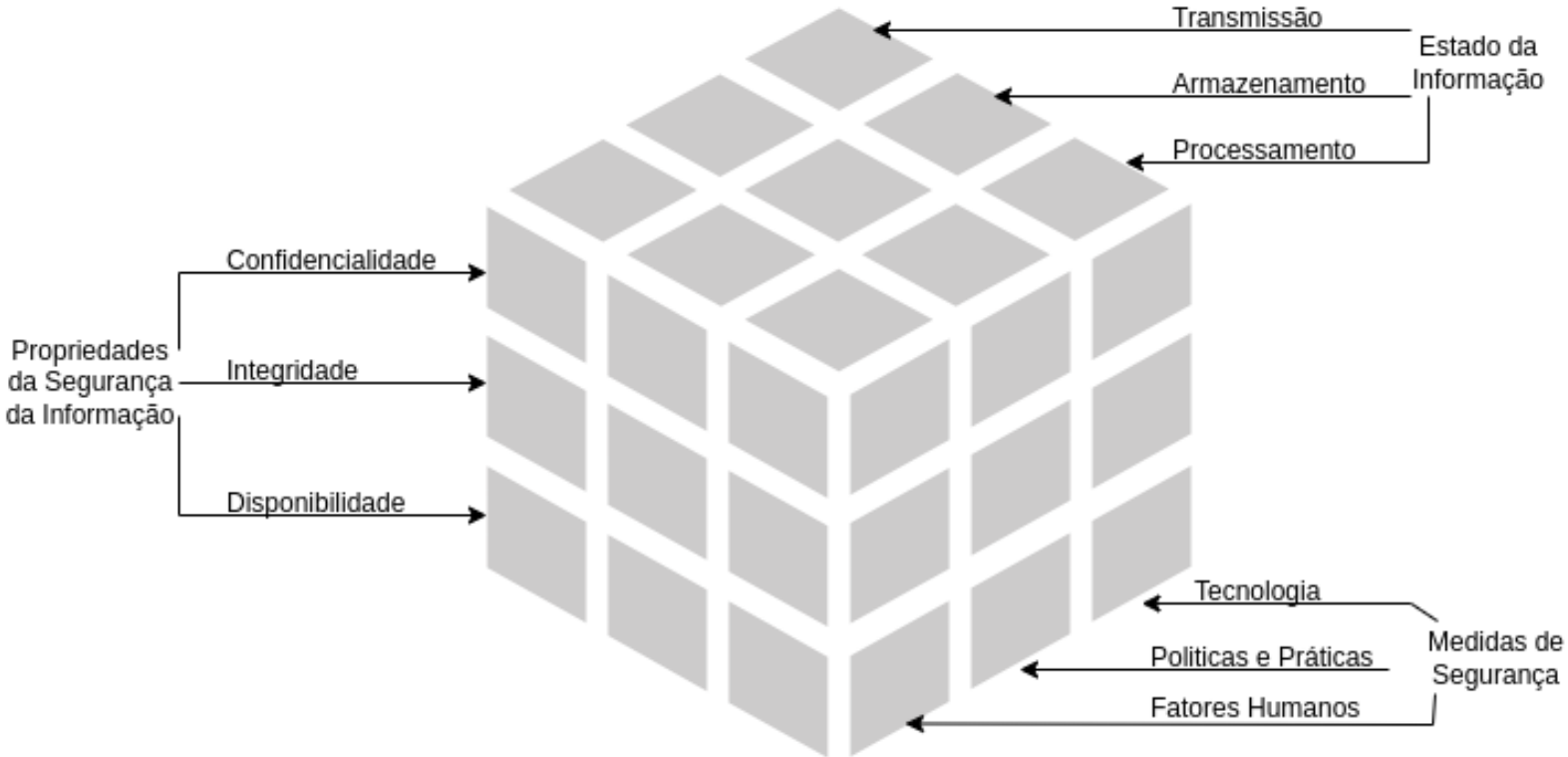
Cubo de McCumber



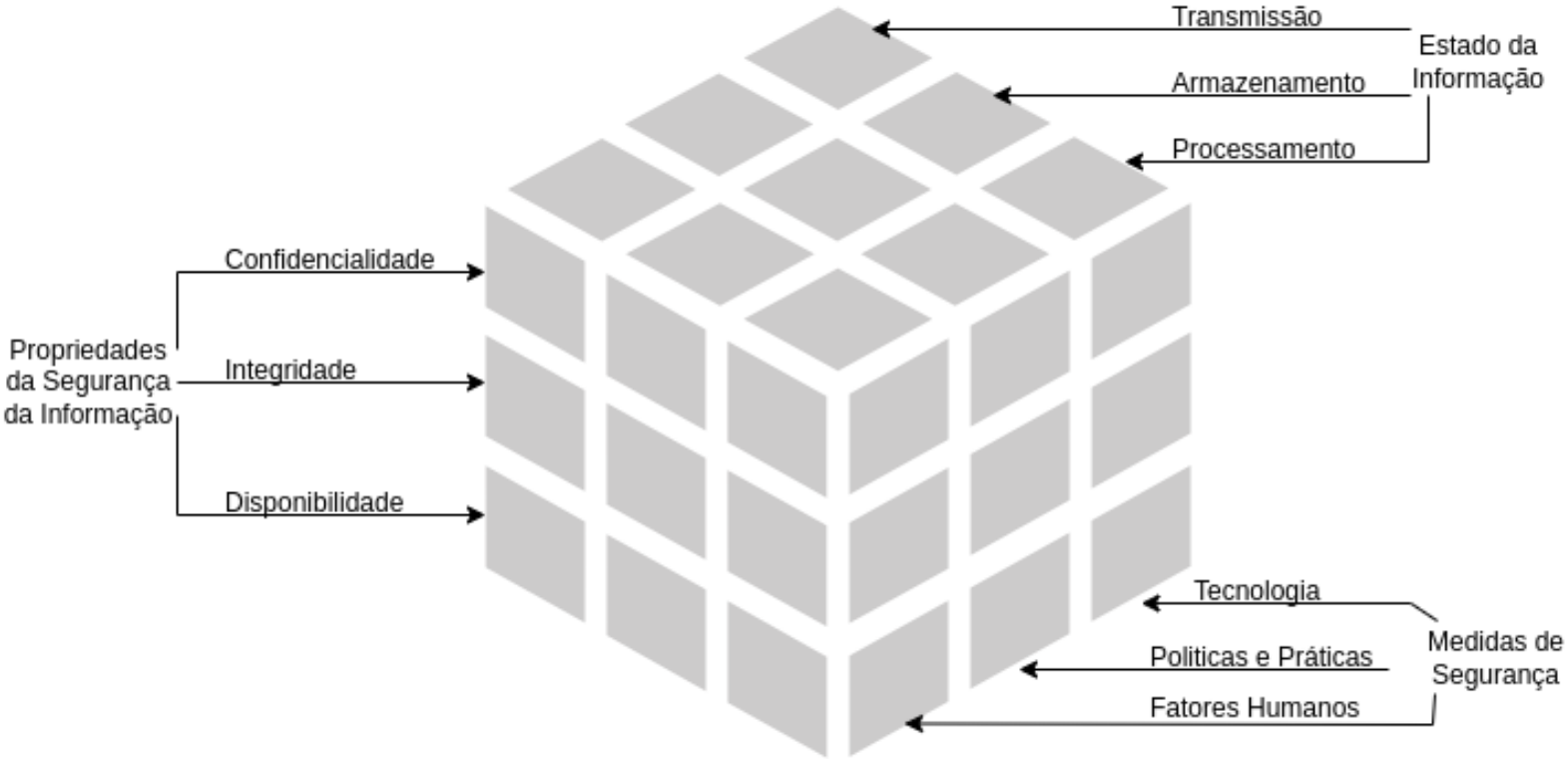
Processamento

Execução de operações nos dados para alcançar um objetivo.

Cubo de McCumber



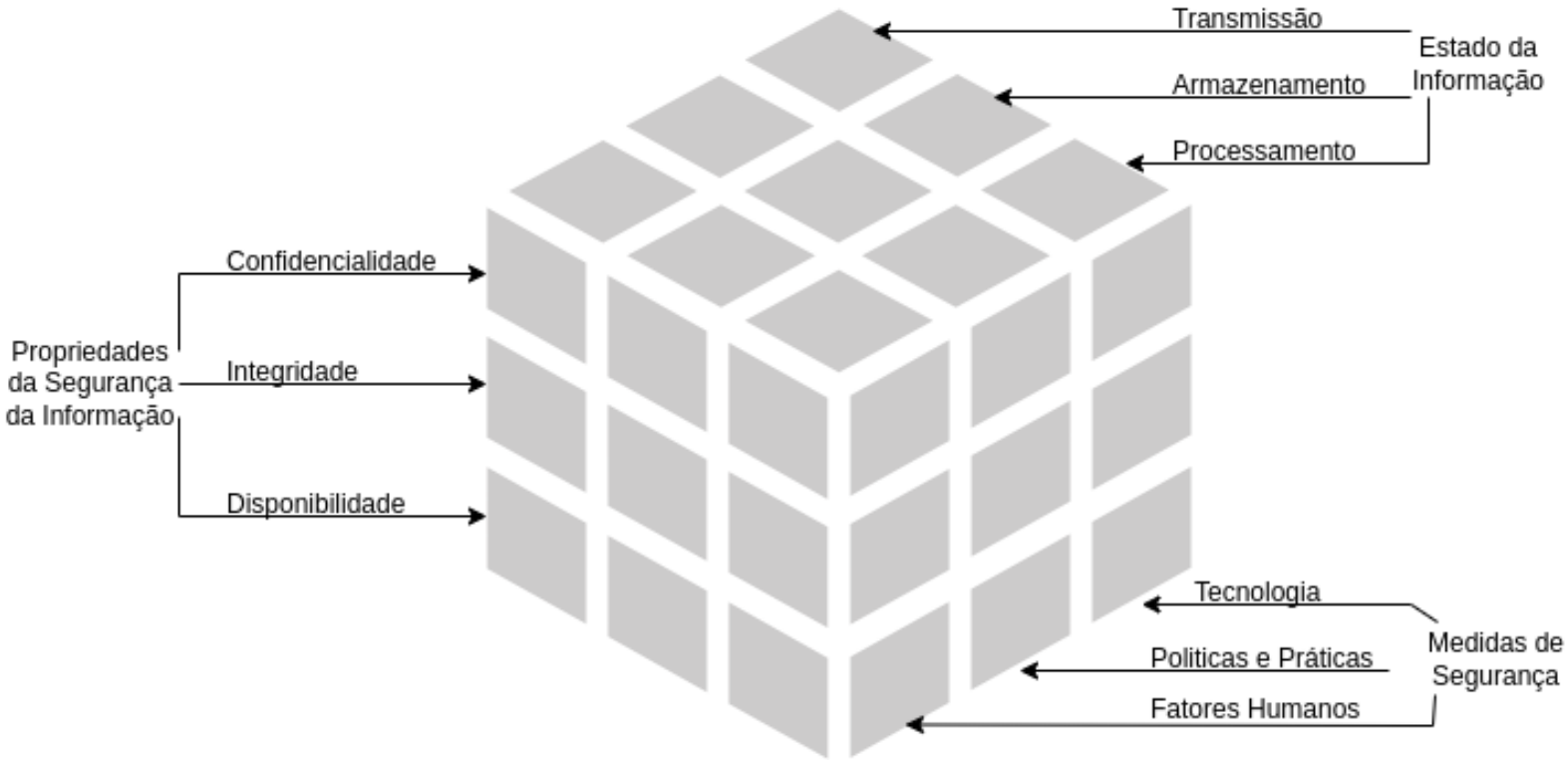
Cubo de McCumber



Tecnologia

Soluções de Hardware e Software desenvolvidas para proteger os Sistemas de Informações.

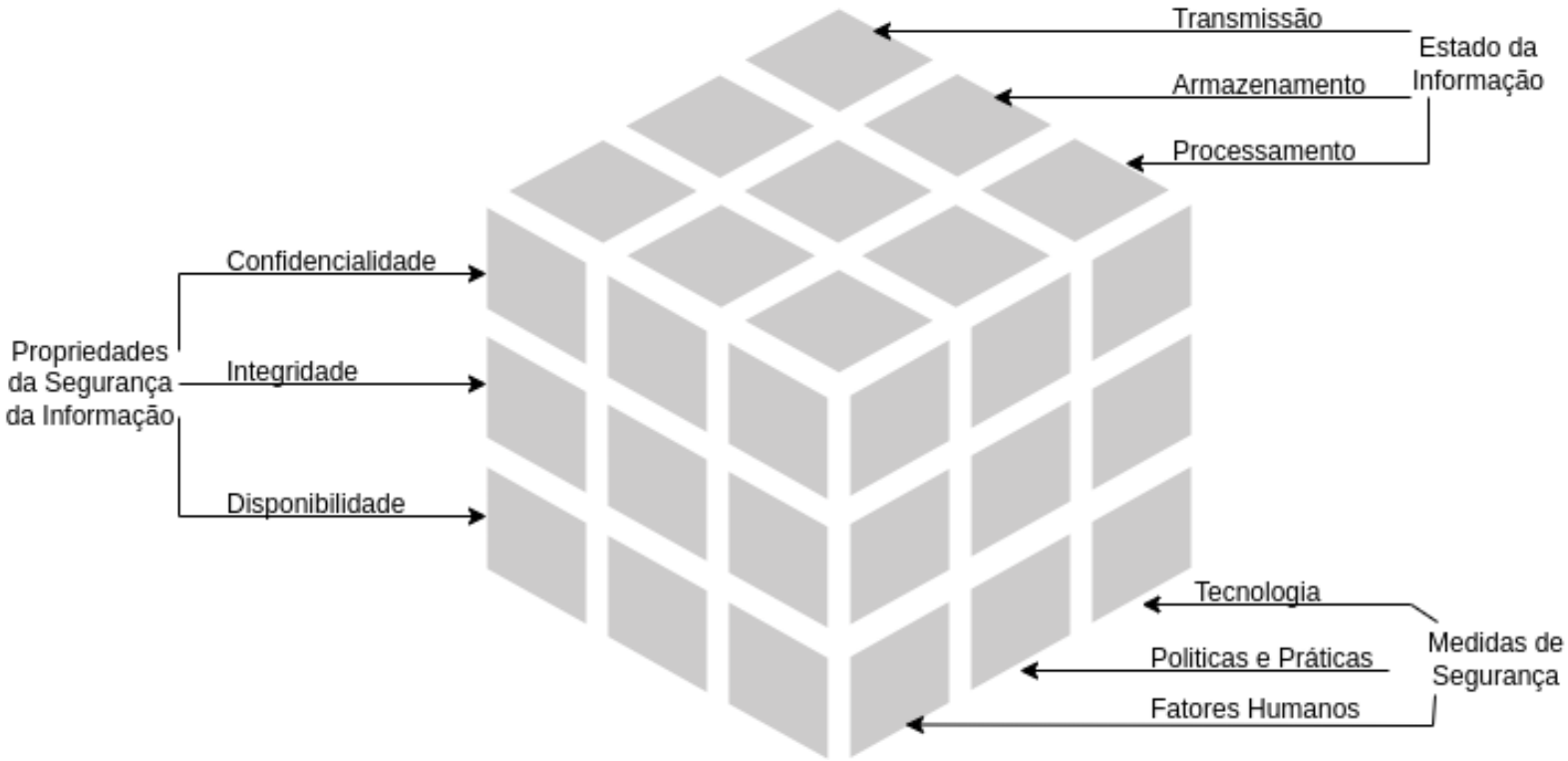
Cubo de McCumber



Politicas e Práticas

Controles administrativos, como diretrizes de gerenciamento, que fornecem uma base de como a garantia da informação deve ser implementada dentro de uma organização.

Cubo de McCumber



Fatores Humanos

Assegurar que os usuários de sistemas de informação estejam cientes de seus papéis e responsabilidades em relação à proteção de sistemas de informação e sejam capazes de seguir padrões.

Segurança dos Dados vs Privacidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Segurança dos Dados

proteção das informações de uma empresa contra acessos maliciosos ou equivocados, sequestro, roubo ou modificação não autorizada de seu conteúdo

Segurança dos Dados vs Privacidade

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

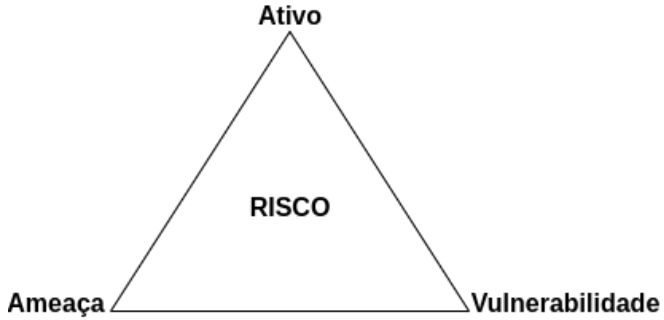
Segurança dos Dados

proteção das informações de uma empresa contra acessos maliciosos ou equivocados, sequestro, roubo ou modificação não autorizada de seu conteúdo

Privacidade de Dados

a capacidade das pessoas determinarem por si mesmas quando, como e até que ponto as informações pessoais sobre elas são compartilhadas ou comunicadas a outras pessoas.

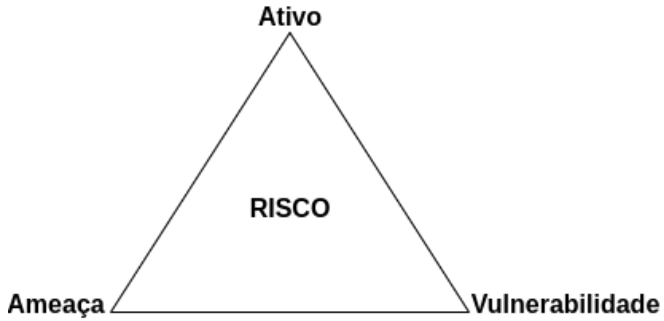
Risco



Ativo

Um ativo é o que estamos tentando proteger.

Risco



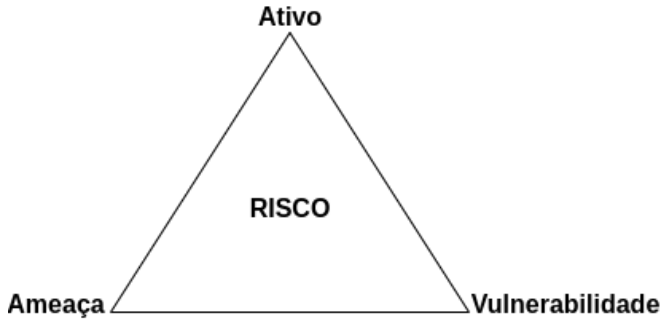
Ativo

Um ativo é o que estamos tentando proteger.

Ameaça

Uma ameaça é contra a qual estamos tentando proteger.

Risco



Ativo

Um ativo é o que estamos tentando proteger.

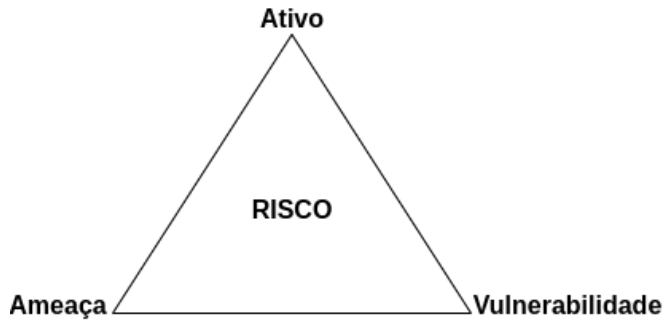
Ameaça

Uma ameaça é contra a qual estamos tentando proteger.

Vulnerabilidade

Uma vulnerabilidade é uma fraqueza ou falha em nossos esforços de proteção.

Risco



Risco

O potencial de perda, dano ou destruição de um ativo como resultado de uma ameaça que explora uma vulnerabilidade. Risco é uma possibilidade de corromper um ativo, através de ameaças e vulnerabilidades.

Componentes de um Sistema de Informação

Sistema de Informação

todo conjunto de pessoas, procedimentos e tecnologia que permite que as empresas usem as informações.

- Os componentes básicos de um sistema de informação são:
  - hardware;
  - software;
  - redes;
  - pessoas;
  - procedimentos;
  - dados.

Tipos de Ataques

- **Engenharia social** - técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações.
- **Varredura em redes (scan)** - consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados.
- **Negação de serviço distribuída (DDoS)** - atividade maliciosa, coordenada e distribuída, pela qual um conjunto de computadores e/ou dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Tipos de Ataques

- **Força bruta** - consiste em adivinhar, por tentativa e erro, um nome de usuário e senha de um serviço ou sistema.
- **Invasão ou comprometimento** - ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.
- **Desfiguração de página (Defacement)** - consiste em alterar o conteúdo da página Web de um site.
- **Escuta de tráfego** - consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos.

Exemplo de Ataque

Controle de Acesso e Correlatos

- **Controle de Acesso** - garantir que recursos só sejam concedidos àqueles usuários que possuem permissão.
  - **Identificação** - permitir que uma entidade se identifique, ou seja, diga quem ela é. Ex.: conta de usuário, conta do banco, e-mail
  - **Autenticação** - verificar se a entidade é realmente quem ela diz ser. Ex.: senha, token, biometria
- **Exemplos**
  - conta de usuário - é a identificação
  - senha - é a autenticação
  - cookies - permitem identificar os acessos que fazem parte de uma mesma sessão.

Criptografia

O que é criptografia?

- **Definição clássica** - Etimologicamente, criptografia é a arte da escrita secreta.
- **Definição moderna** - Criptografia é arte/ciência/engenharia que estuda técnicas para fornecimento de serviços de segurança, como sigilo, autenticação de origem, anonimato, integridade e irretratabilidade, primordialmente em sistemas computacionais.

Criptografia

- **chave** - similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos.
- **certificado digital** - registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. É emitido por uma autoridade certificadora.
- **assinatura digital** - código usado para comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada.

Proteção de dados em Trânsito

- **SSL/TLS, SSH e IPSec** - protocolos que, por meio de criptografia, fornecem confidencialidade e integridade nas comunicações entre um cliente e um servidor.
- **VPN** - termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Em geral utilizam criptografia e outros mecanismos de segurança para proteger os dados em trânsito.
  - Existem serviços na Internet que dizer fornecer uma VPN, mas que apenas fornecem serviços de proxy que "ocultam"o IP de origem - a maior parte destes serviços não cifra o conteúdo em trânsito.

- **PGP** - programa que implementa operações de criptografia, como cifrar e decifrar conteúdos e assinatura digital.
  - Normalmente utilizado em conjunto com programas de e-mail.

Registros de Eventos (Logs)

- São os registros de atividades gerados por programas e serviços de um computador. A partir da análise destas informações é possível:
  - detectar problemas de hardware ou nos programas e serviços instalados no computador;
  - detectar um ataque;
  - detectar o uso indevido do computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema.

Ferramentas contra comprometimentos

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Firewall** - usado para dividir e controlar o acesso entre redes de computadores.
  - um firewall só pode atuar no tráfego que passa por ele
  - quando o firewall é instalado para proteger um computador é chamado de firewall pessoal

- Opera com base em regras pré-definidas
  - Mais comum: com base nas informações dos cabeçalhos IP, TCP, UDP, etc
  - Firewall de aplicação - nome dado quando a filtragem é feita com base na análise do conteúdo "assinaturas" de ataques

Ferramentas contra comprometimentos

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- **Antimalware** - procura detectar e, então, anular ou remover os códigos maliciosos de um computador.
  - Os programas antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas antimalware.

- **Filtro antispam** - permite separar os e-mails conforme regras pré-definidas.
  - Pode ser implementado com base em análise de conteúdo ou de origem das mensagens.

Detecção de Atividades Maliciosas

- **IDS** - programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas
  - geralmente implementado com base na análise de logs ou de tráfego de rede, em busca de padrões de ataque pré-definidos.

- **Fluxos de rede (Flows)** – sumarização de tráfego de rede
  - armazena IPs, portas e volume de tráfego
  - permite identificar anomalias e perfil de uso da rede
  - em segurança usado para identificar:
    - ataques de negação de serviço
    - identificar computadores comprometidos

Resiliência Operacional

- Um sistema 100% seguro é muito difícil de atingir
- Para conseguir uma segurança razoável tem-se tentado atingir os seguintes objetivos:
  - Detectar comprometimentos o mais rápido possível
  - Diminuir o impacto - Conter, mitigar e recuperar de ataques o mais rápido possível
- Novo paradigma: Resiliência
  - Continuar funcionando mesmo na presença de falhas ou ataques

Como Obter Resiliência?

- Identificar o que é crítico e precisa ser mais protegido
- Definir políticas (de uso aceitável, acesso, segurança, etc)
- Treinar profissionais para implementar as estratégias e políticas de segurança
- Treinar e conscientizar os usuários sobre os riscos e medidas de segurança necessários
- Implantar medidas de segurança que implementem as políticas e estratégias de segurança
  - como aplicar correções ou instalar ferramentas de segurança
- Formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes

Bibliografia

- Adaptado de Cristine Hoepers - https://www.cert.br/docs/palestras/certbr-egi2014.pdf
- Cartilha de Segurança para a Internet - http://cartilha.cert.br/
- WHITMAN, Michael E.; MATTORD, Herbert J. Principles of information security. Cengage learning, 2021.

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM