Ciência da Computação Integrada

(Apresentação do Power Point)

1.Dados, Informação, Conhecimento, Sabedoria

•. O que são **dados**?

São sinais que não foram processados, correlacionados, avaliados ou interpretados. Isoladamente não podem transmitir uma mensagem ou representar algum conhecimento. (Matéria-Prima a ser utilizada na produção de informações).

•. O que é **informação**?

Informações são dados tratados. O processo de transformação envolve a aplicação de procedimentos como formatação, tradução, fusão, impressão e assim por diante.

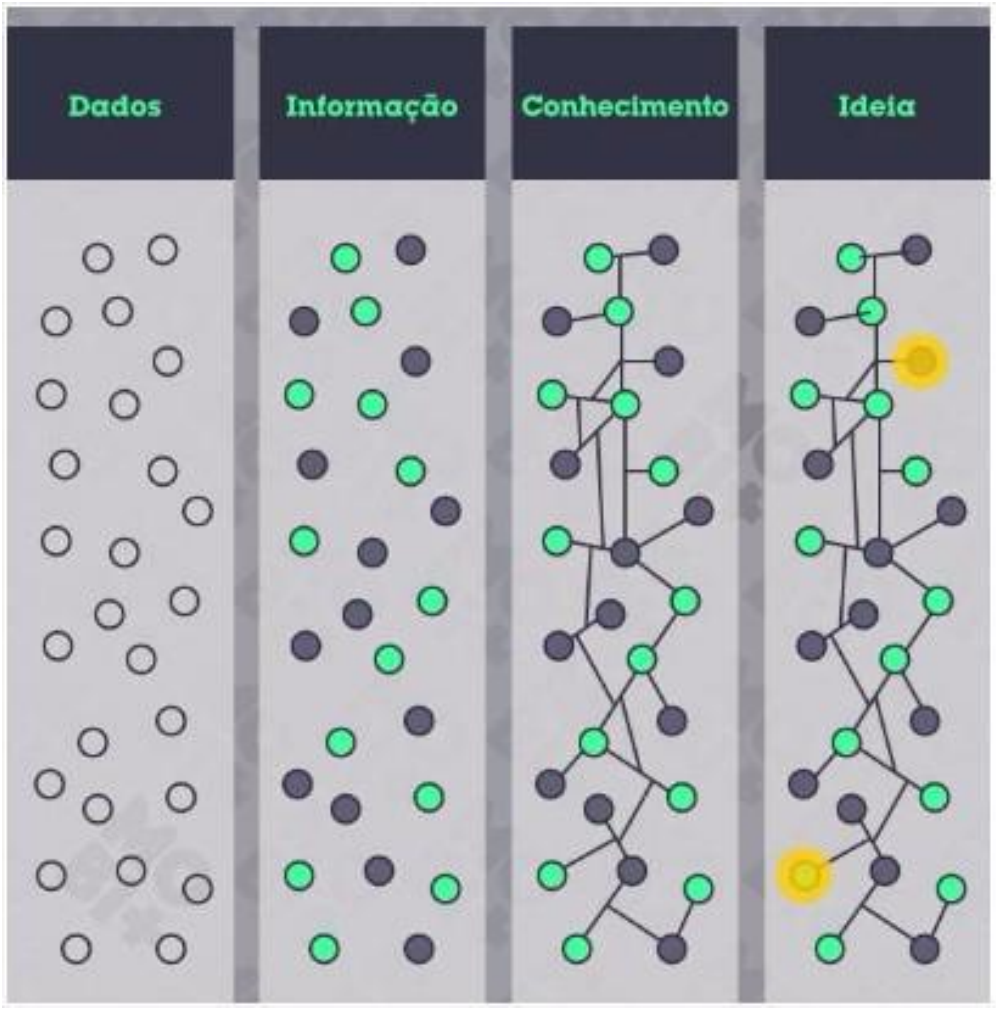
As informações têm significado e podem ser utilizadas para tomada de decisões.

•. O que é **conhecimento**?

"Informações que foram analisadas e avaliadas sobre a sua confiabilidade, sua relevância e sua importância" (DAVENPORT, 2000). É obtido pela interpretação e integração de vários dados e informações. É a informação contextualizada.

•. O que é **sabedoria**?

Pode ser vista como uma extensão do conceito de conhecimento. Na verdade, ela é o conhecimento acrescido de ética e valores.



1.1. Informação

"A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida".

•. Valor da informação:

Não é mais possível obter grandes lucros fazendo ou movimentando coisas, nem mesmo controlando dinheiro. Recursos tradicionais (mão de obra, terra, capital) produzem

retornos cada vez menores, e os maiores produtores de riqueza passaram a ser a informação e o conhecimento.

Peter Drucker.

1.2. A Era da Informação

- Era da Informação (também conhecida como Era Digital) é o nome dado ao período que vem após a Era Industrial, mas especificamente após a década de 1980, embora suas bases tenham começado no início do século XX com invenções como o microprocessador, rede de computadores, a fibra óptica e o computador pessoal.

•. 4ª Revolução Industrial:

- É caracterizada por mudanças abruptas e radicais, motivadas pela incorporação de tecnologias, tendo desdobramentos nos âmbitos econômico, social e político.

- Inovações tecnológicas vão mudar radicalmente o mundo como o conhecemos e moldar a indústria dos próximos anos.

•. As Revoluções Industriais

- A **primeira** aconteceu entre 1760 e 1840, movida por tecnologias mecânicas como máquinas a vapor e as ferrovias.

- A **segunda** aconteceu entro o final do século XIX e meados do século XX, tendo como principal inovação a eletricidade e seu emprego em bens de consumo e eletrodomésticos, a linha de montagem e a difusão da produção em massa.

- A **terceiram,** que se iniciou na década de 1960, é o advento da informática e da tecnologia da informação, o uso de computadores pessoais e, mais tarde, nos anos 1990, a internet e as plataformas digitais. Tecnologias robóticas, inteligência artificial, realidade aumentada, big data, nanotecnologia, impressão 3D e a chamada Internet das coisas.

2.Tecnologia da Informação

Tecnologia da Informação é a área de conhecimento responsável por criar, administrar e manter a gestão da informação através de dispositivos e equipamentos para acesso, operação e armazenamento dos dados, de forma a gerar informações para tomada de decisão.

TI provoca repercussão em todos os níveis da estrutura organizacional:

- No nível estratégico, que se traduz em um aumento de eficácia em termos de cumprimento da missão organizacional.

- Nos níveis operacionais e administrativos, que se traduz em aumento da eficiência organizacional.

•. TI poder:

- Provocar alterações nas condições competitivas de determinado mercado.

- Provocar dissuasão e criação de barreiras à entrada de novos concorrentes.

- Desenvolver novos produtos/serviços aos clientes ou diferenciar os já existentes dos da concorrência e que atraem o cliente de forma preferencial em relação a concorrência.

3.Períodos da TI

•. **A era do Processamento de Dados**

- Em **1960** os computadores começaram a se tornar importantes para as grandes e médias empresas, mas eram limitadíssimos quanto a aplicações e incompatíveis entre si.

- Em **1970**, as linhas telefônicas passaram a permitir o acesso a terminais remotos de computadores e as telecomunicações se tornaram uma base tecnológica.

- Toda a ação acontecia na sala de processamento de dados chamados **CPD's (Centro de Processamento de Dados)** responsáveis pelo tratamento das informações, onde o acesso a esse volume de dados era realizado por relatórios gerados pelo sistema ou terminais ligados ao computador central.

•. **A era dos Sistemas de Informações**

- Em **1970** as transformações tecnológicas começaram a abrir novas opções para a transformação de dados em informações e ao melhoramento e adequação dos sistemas de acordo com as necessidades da empresa.

- O terminal, pela primeira vez, se torna flexível.

- Surgem também os pacotes de software.

•. **A era da Inovação e Vantagem Competitiva**

- Em 1980, mudanças tecnológicas principalmente em tecnologias de escritório e microcomputadores, e o termo "Tecnologia da Informação" passou a ser mais usado.

- Gerenciadores de banco de dados se tornaram disponíveis nos PCs e softwares de custo baixo dominaram o mercado.

- Mesmo com todos os avanços da época, como as redes locais, os computadores ainda eram incompatíveis entre si, dificultando assim a integração dos sistemas e uma maior flexibilidade. A busca pela descentralização se torna mais forte.

•. A era da Integração e Reestruturação do Negócio

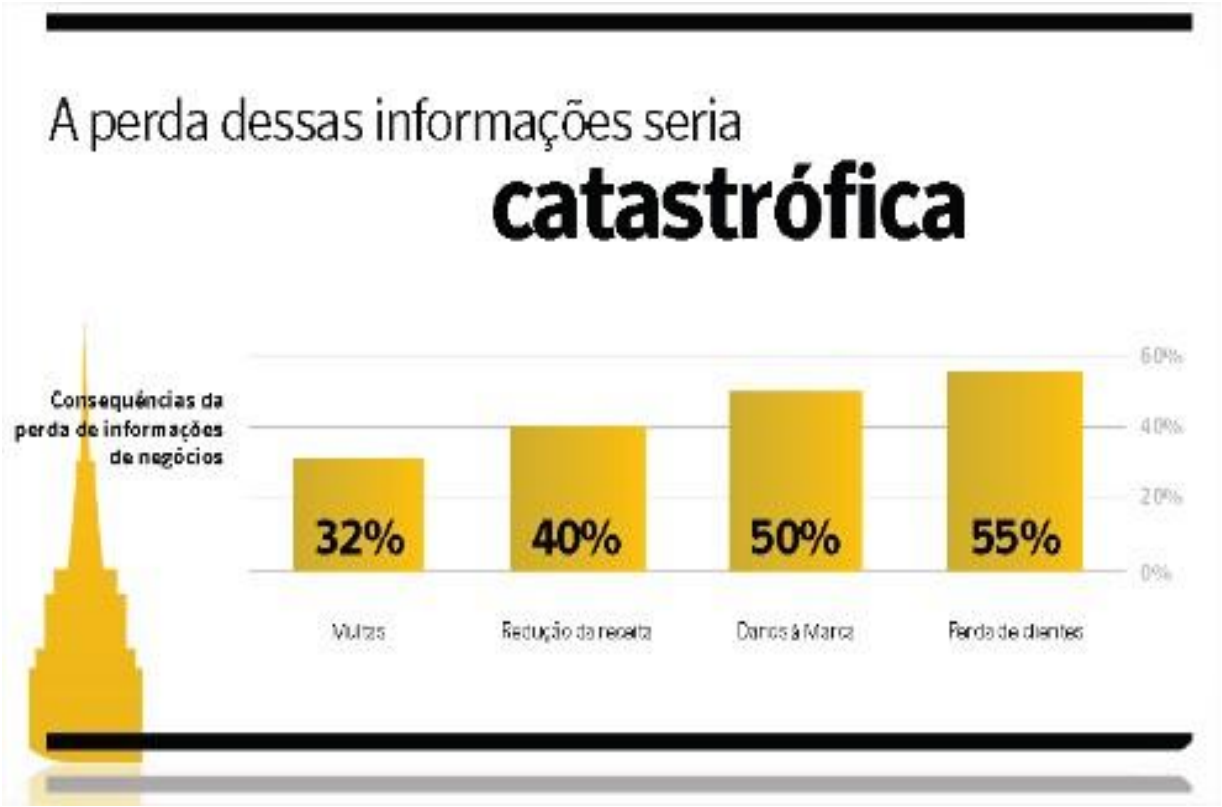
- Em 1990, sistemas abertos, integração e modelos se tornam itens essenciais nos departamentos de sistemas acabando com incompatibilidade. A integração tecnológica flexibilizou e facilitou a troca e o acesso às informações otimizando o funcionamento da empresa.

4.Segurança da Informação – SI

A segurança da informação está relacionada com proteção de conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

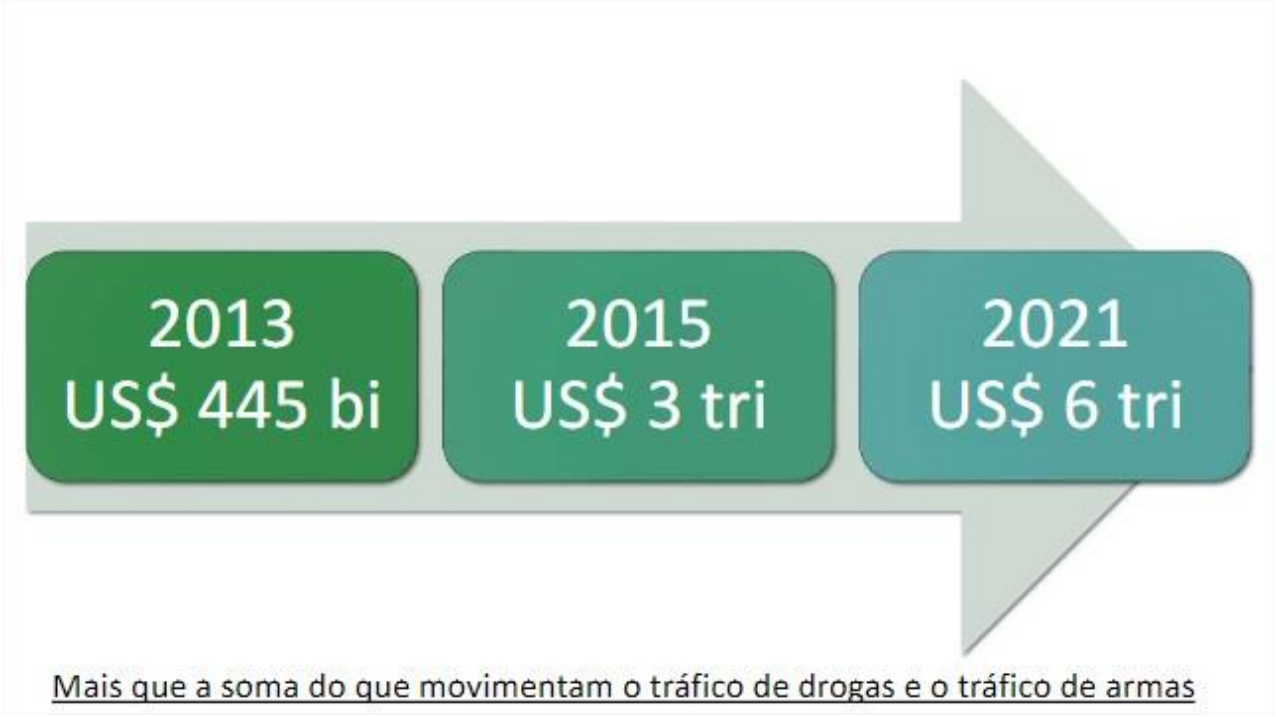
•. Quanto vale a informação?

•. Quanto custa a perda?



Multas/ Redução da receita/ Danos à marca/ Perda de cliente

•. Mercado do Cibercrime

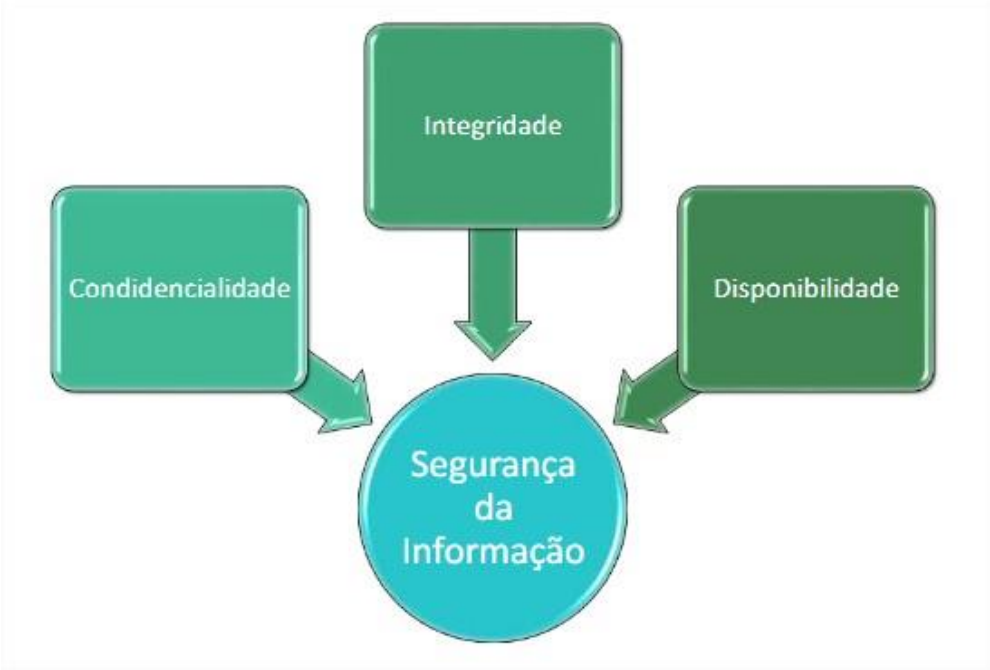


5.Características da SI

São características básicas da segurança da informação os atributos de CID:

✓ Confidencialidade

✓ Integridade



✓ Disponibilidade

5.1. Pilares da SI

•. **Confidencialidade:** Garantir que a informação seja acessível somente por quem possui autorização do proprietário da informação para acessar.

•. **Integridade**: Garantir a salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

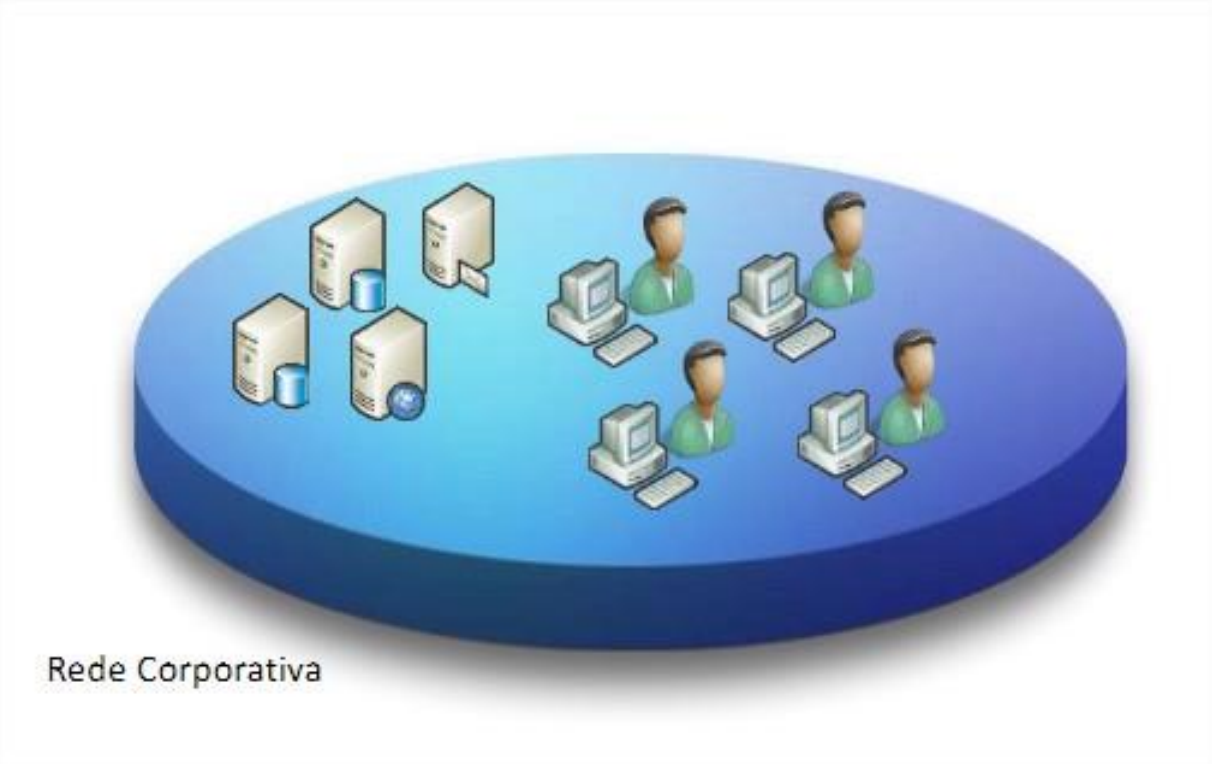
•. **Disponibilidade:** Garantir que a informação esteja sempre acessível e disponível quando necessário, por aqueles usuários autorizados.

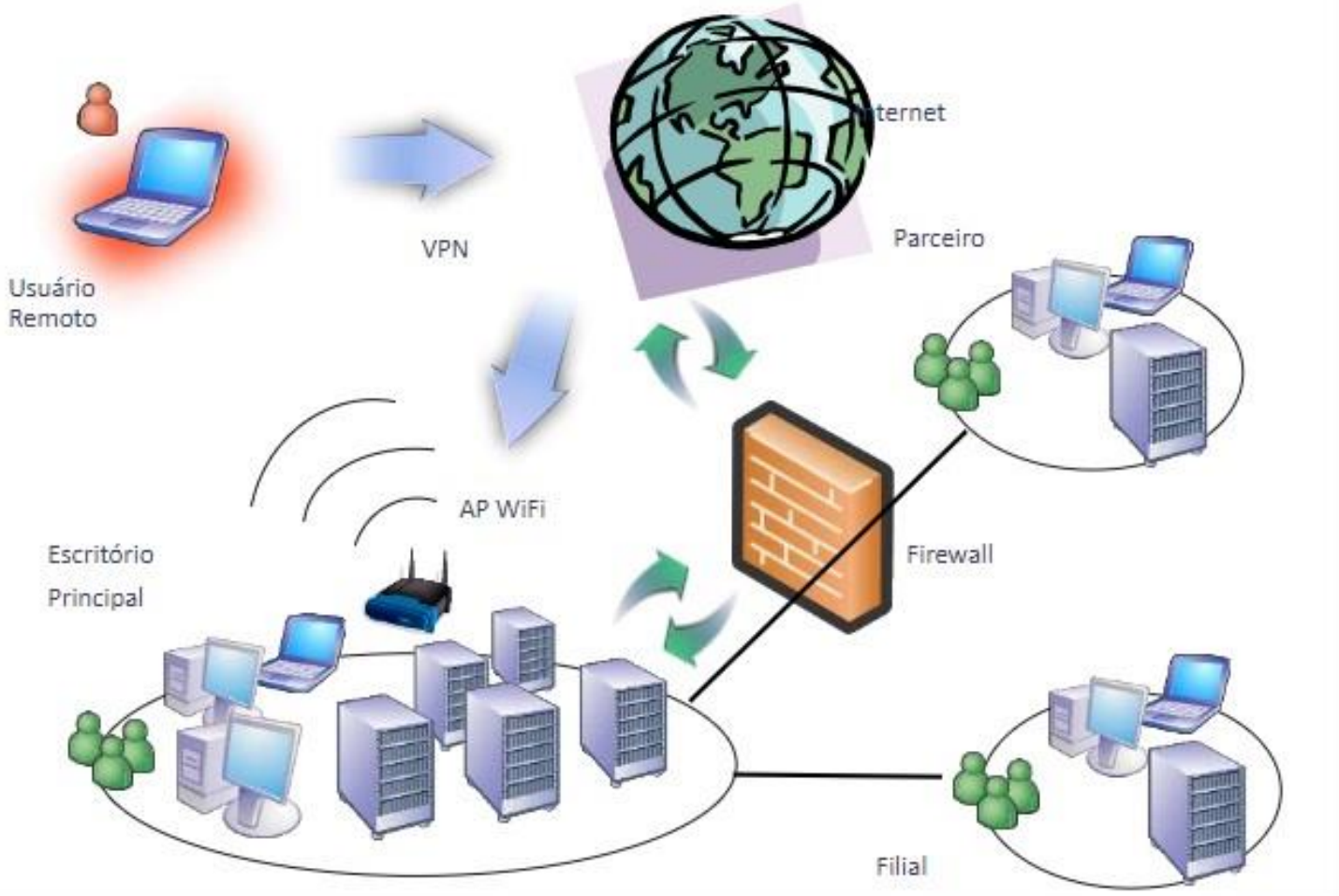
Outros atributos:

•. **Autenticidade:** Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

•. **Irretratabilidade:** Propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

•. <u>Conformidade:</u> Propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.





6.Segurança da SI

- A maior dificuldade em implementar segurança não é tecnológica, e sim organizacional.

6.1. Governança de TI

As empresas estão sacrificando dinheiro, produtividade e vantagem competitiva por não implementar uma governança de TI eficaz.

Os executivos precisam de uma maneira melhor de:

•. Dirigir a TI para obtenção de benefícios

•. Medir o valor fornecido pela TI.

•. Gerenciar os riscos pertinentes a área de TI.

Governança Segurança da Informação

É o conjunto de processos, controles e demais atividades com o propósito de garantir:

✓ A gestão do programa corporativo de segurança da informação está orientada aos objetivos de negócio.

✓ Exista uma avaliação contínua das políticas, padrões, procedimentos e riscos em segurança da informação.

✓ Os riscos em segurança da informação estejam em níveis aceitáveis pela organização.

Gestão de Segurança da Informação

A gestão cuida da execução eficiente e eficaz das atividades previstas para o processo de segurança. Ela tem como objetivo garantir a existência de controles para a proteção da informação, em todas as dimensões existentes, necessárias para a realização do negócio e alcance dos objetivos do negócio da Organização.

A gestão é o como fazer a segurança da informação.

Sustentabilidade de Segurança da Informação

Sustentabilidade do processo de segurança da informação é o conjunto de ações e decisões que devem existir para que este processo:

✓ Seja continuo ao longo do tempo.

✓ Permita que este processo se retro alimente.

✓ Permita que a organização aprenda.

✓ Possibilite que as perdas e impactos que o processo de segurança impediu que a organização sofresse, tornem-se os geradores de recursos para o patrocínio deste processo.

Sem dúvida alguma o apoio da alta direção da Organização e o alinhamento aos objetivos de negócio são críticos para que haja esta sustentabilidade.

Governança ~ O que se quer: Priorização

Gestão ~ Como fazer acontecer o que se quer

Sustentabilidade ~ Como garantir que, o que se quer, será alcançado sempre ao longo do tempo.

7.TIL

Conjunto de melhores práticas que orientam o gerenciamento de serviços de TI.

Consiste em uma série de publicações que fornecem recomendações para o provisionamento da qualidade dos serviços de ti e dos processos e recursos necessários para suporta-los.

Trata de "como" fazer os serviços de TI.

5 volumes:

1) Estratégia de Serviço

2) Desenho Serviço

3) Transição de Serviço

4) Operação de Serviço

5) Melhoria Continua de Serviço

Proporciona uma série de benefícios às empresas:

✓ Aumento da satisfação dos clientes em relação aos serviços prestados pela TI.

✓ Aumento da disponibilidade dos serviços, levando diretamente a aumento dos lucros e resultados.

✓ Economia advinda da redução de trabalho, tempo perdido, melhoria do gerenciamento e uso de recursos.

✓ Melhoria do tempo de disponibilização de novos produtos e serviços.

✓ Melhoria da tomada de decisão e otimização de riscos.

8.CoBIT

Conjunto de Ferramentas que garante que a área de TI está trabalhando efetivamente.

Funciona como um framework abrangente.

Baseado em boas práticas em:

- Alinhamento estratégico da TI com os objetos de negócio.

- Valor dos serviços prestados e novos projetos.

- Gerenciamento de risco.

- Gerenciamento de recursos.

- Gerenciamento de desempenho.

Trata "do que" fazer nos serviços de TI.

Princípios do Cobit 5:

✓ Satisfazer as necessidades das partes interessadas;

✓ Envolver todas as áreas da empresa;

✓ Empregar uma estrutura única e integrada;

✓ Possibilitar uma abordagem holística;

✓ Separar governança de gerenciamento.

9.ISO 20.000

É um conjunto que define as melhores práticas de gerenciamento de serviços de TI, e tem a intenção de ser completamente compatível com o ITIL.

São requisitos da norma definição de políticas, objetivos, procedimentos e processos de gerenciamento para assegurar a qualidade efetiva na prestação de serviços de TI.

Os processos da ISO/IEC 20.000 são os seguintes:

✓ Processos de planejamento e implementação (PDCA)

✓ Processos de entrega de serviços.

✓ Processos de relacionamento.

✓ Processos de solução, liberação e controle.

•. Série ISSO 27.000

Estão muito relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos.

Exemplos:

ISO 27.000 – Traz informações básicas sobre as normas da série.
ISO 27.001 – Bases para a implementação de um SGSI em uma organização.
ISO 27.002 – Certificação profissional, traz códigos de práticas para profissionais (apresenta 133 controles para a Política de Segurança da Informação).
ISO 27.003 – Diretrizes mais específicas para implementação do SGSI.
ISO 27.004 – Normas sobre as métricas e relatórios do SGSI.
ISO 27.005 – Norma sobre gestão de riscos do SGSI.
ISO 27.017 – Controles Computação em Nuvem
ISO 27.033 – Segurança de Redes (6 partes)
ISO 27.037: orientações para a identificação, coleta, aquisição e preservação de evidências forenses digitais.

10. Agentes da SI

✓ **Gestor da Informação**

Área responsável pela informação. Cabe ao gestor classificar a informação e deliberar sobre as proteções que deverão ser aplicadas aos seus ativos de informação.

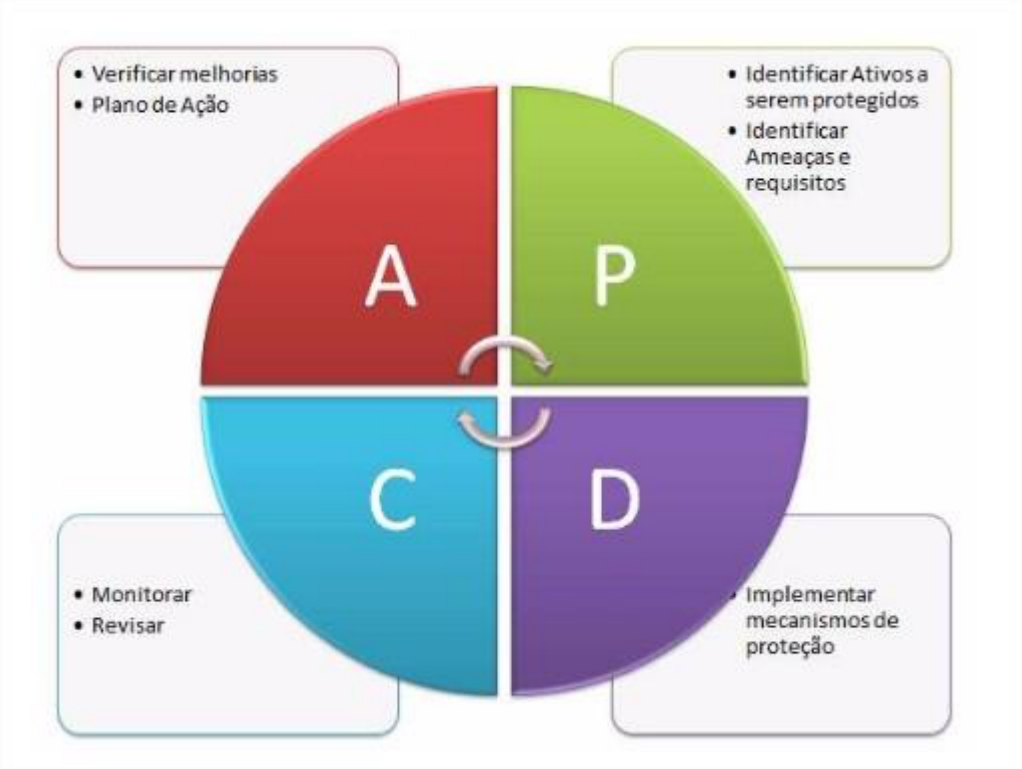
✓ **Custodiante**

Responsável pelo processamento, organização e guarda da informação. Normalmente a área de TI.

✓ **Usuário**

Pessoa que interage diretamente com a informação em suas diversas formas.

• **Ciclo de Segurança**



1) Primeira Etapa:

2) Segunda Etapa

3) Terceira Etapa

4) Quarta Etapa

A implementação de uma política de segurança da informação segue o modelo do ciclo PDCA onde temos quatro passos:

1. Planejar (Plan): Neste passo devemos identificar os ativos a serem protegidos através da análise de riscos;

2. Realizar (Do): Uma vez definido os ativos a serem protegidos, bem como as ameaças, devemos colocar em ação o planejamento realizado e aplicar os mecanismos necessários para atender os requisitos de proteção identificados.

3. Verificar (Check): Após a implementação do plano através do passo anterior, devemos monitorar se o plano está sendo seguido e se necessita ser revisado.

4. Agir (Act): Após a monitoração e revisão, é necessário ter um plano de ação para reiniciar o ciclo e planejar mudanças na política estabelecida no plano anterior.

11. Malwares

•. **Vírus**

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo nos sistemas afetados, ou tornando-se parte de outros programas e arquivos de um computador. O vírus depende de uma ação do usuário para se tornar ativo e infectar.

•. **Worms**

É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Não necessita ser explicitamente executado na máquina para se propagar. Sua propagação é através da exploração de vulnerabilidades existentes.

•. **Trojan Horses**

É um programa normalmente recebido como um "presente", que além de executar funções para as quais foi aparentemente projetado, também executa outras informações normalmente maliciosas e sem o conhecimento do usuário.

•. **Spywares**

Refere-se a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar

informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

- **Spam e Phishing**

SPAM: e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Phishing: mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros, ao acesso de páginas fraudulentas na internet ou a instalação de códigos maliciosos.