


# SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

**Prof. Cesar Amaral**  
**prof.cesar.amaral@gmail.com**

# Aula 1 - Informações corporativas e a evolução do ambiente computacional, CIDAL e Ciclo de vida da informação

A series of horizontal lines in teal and white, with varying lengths and thicknesses, extending from the left edge of the slide towards the right.

# Informações corporativas e a evolução do ambiente computacional

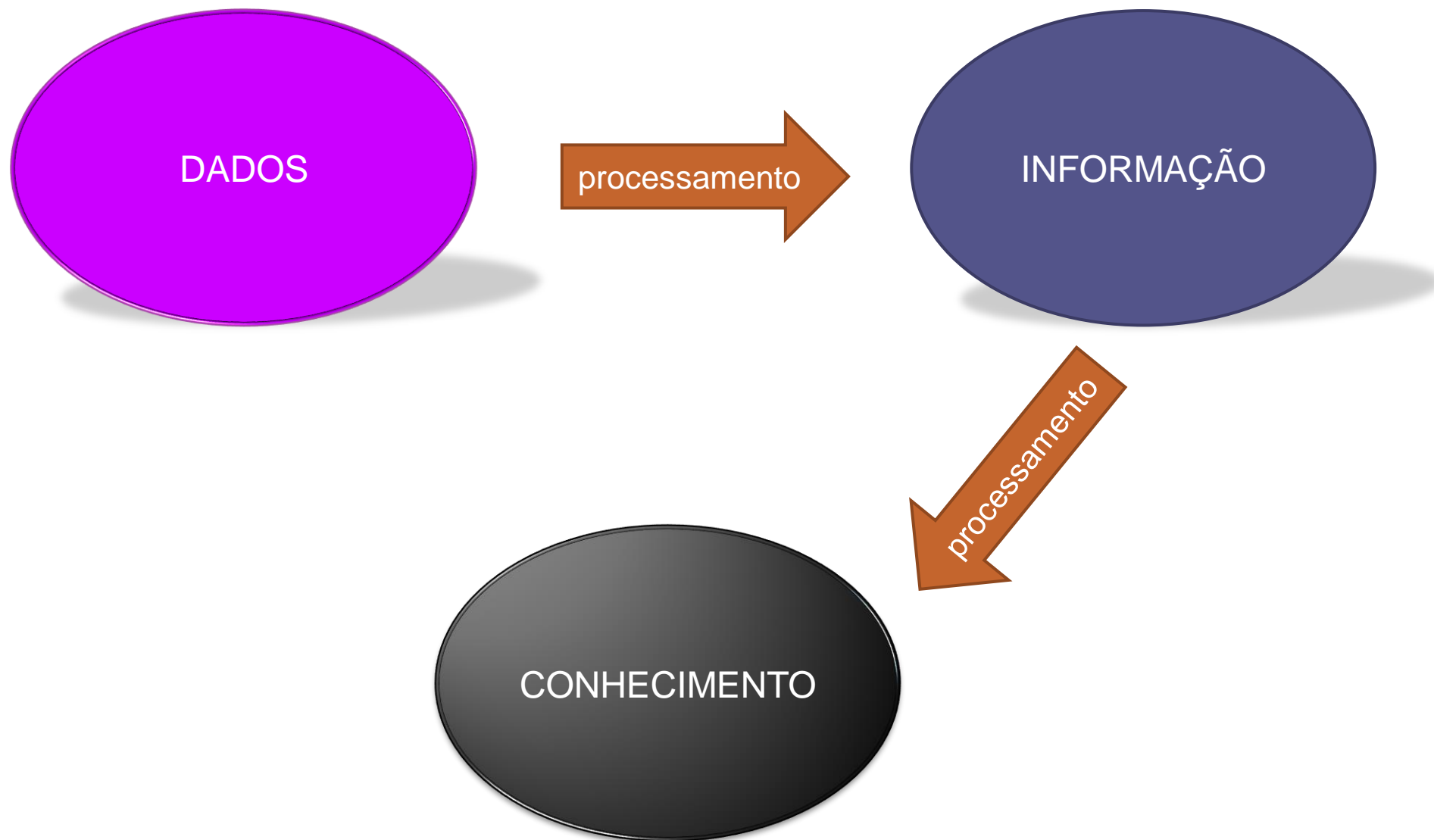
- Atualmente, as empresas se tornaram globais, atuando no mundo inteiro e tendo suas transações sendo efetuadas com cada vez maior velocidade transações.
- Isso graças às redes de computadores e a internet, que permitem a comunicação on-line e real time.
- Hoje em dia uma empresa aqui no Brasil troca informações e se comunica com sua matriz no Japão como se estivessem lado a lado.

- Com isso, a informação passou a ser o ativo mais importante da empresa, e passou a ser alvo de preocupações por parte das empresas quanto a seu uso, acesso, compartilhamento, preservação, espionagem, etc.
- As empresas estão muito dependentes de suas informações!!! Qualquer informação perdida pode representar um grande prejuízo para os negócios...
- As transações das empresas ficaram mais rápidas e organizadas, aumentando seus lucros.

- Quando a informação estava armazenada em papel, bastava um armário com chave e uma sala bem fechada e pronto, a informação estava segura. Só tinha acesso à informação quem devia!
- Hoje em dia não... A informação está em meio digital em sua maior parte, distribuída em diversos tipos de dispositivos, tornando sua proteção mais difícil.
- A fronteira das empresas vai além de seus muros. A informação pode estar em qualquer lugar, tornando seu gerenciamento e segurança mais complexos.

# DADOS E INFORMAÇÃO

- Dados
  - Bits e bytes manipulados pelo computador
  - Aquilo que, sozinho, não faz sentido
- Informação
  - Dado processado
  - Tem valor, faz sentido
- Exemplo:
  - Dado: 7
  - Informação: José da Silva – nota 7



- Uma empresa lida com milhares de terabytes de informações e informações diariamente, sendo que essa informação é manipulada constantemente.

**1 terabyte (TB) é igual a 1.000 gigabytes (GB) ou 1 milhão de megabytes (MB)**

- Existe uma grande necessidade de se implementar controles que possam permitir às pessoas trabalhar com esses dados e informações de forma segura, e isso é altamente complicado e trabalhoso.



# SEGURANÇA DA INFORMAÇÃO

- Segurança é um “sentimento” que deve haver nas empresas. Os funcionários devem sentir que precisam dela, para que colaborem adequadamente com os controles impostos.
- As pessoas só cuidam daquilo que é importante para elas, e convencer o usuário da importância da informação é bem complicado.
- Vemos nas empresas um cenário em que os usuários não tem grande preocupação com a informação que ele manipula, mas quando se trate da informação dele (pessoal) ele tem grande cuidado.

- Mesmo as empresas, até bem pouco tempo, não tinha grande preocupação com segurança da informação, agindo sempre de maneira corretiva.
- Isso só mudou depois dos ataques de 11 de setembro de 2001, quando as Torres Gêmeas foram derrubadas. Muitas das empresas que estavam lá deixaram de existir, pois toda a informação que elas tinham estavam lá, e sem essa informação foi impossível retomar suas atividades.

# SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

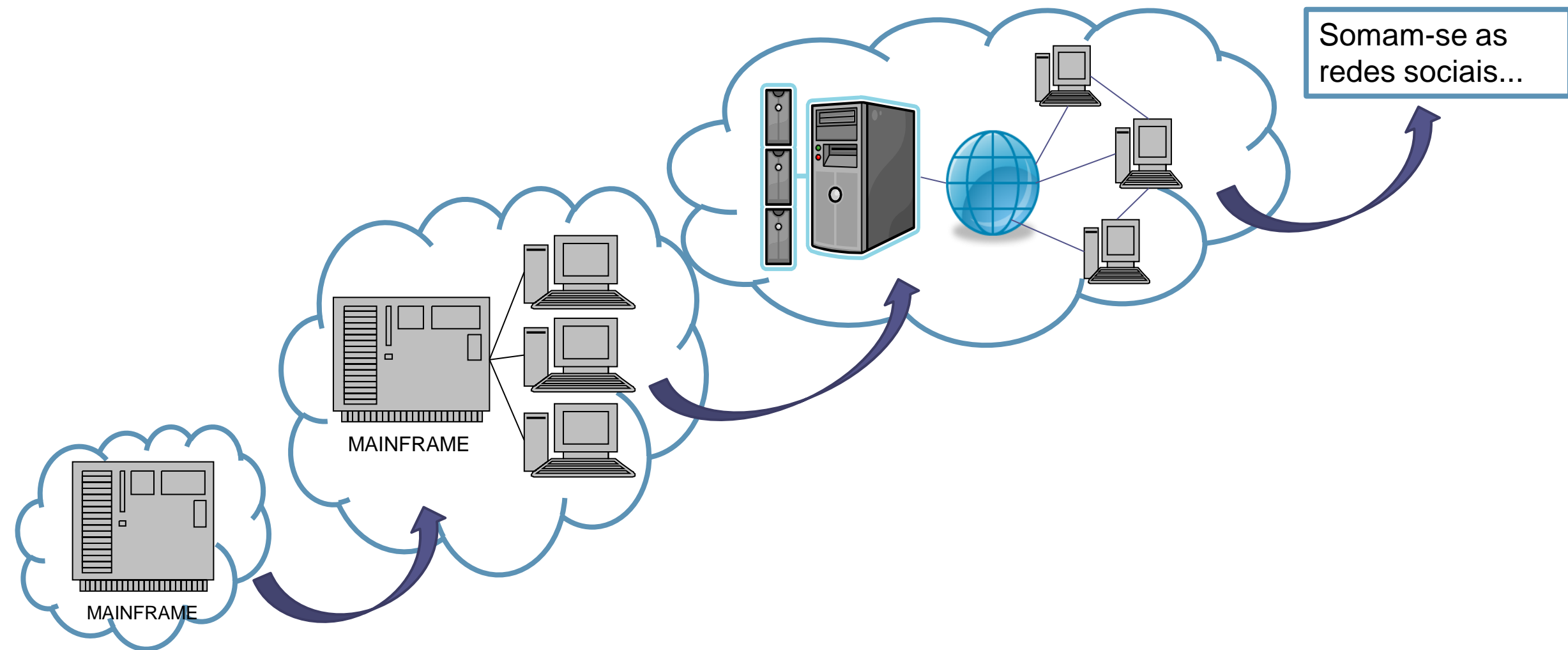
Procedimentos de segurança aplicam-se a qualquer tipo e tamanho de empresa, desde a cafeteria da esquina até a multinacional com ações em bolsas de valores no mundo todo.

# EVOLUÇÃO DO USO DE COMPUTADORES NAS EMPRESAS

- Computadores atuavam isolados uns dos outros e tínhamos os computadores de grande porte (mainframes), com acesso apenas de pessoal altamente qualificado e necessidade de segurança apenas para manter os curiosos afastados.
- Computadores diminuíram de tamanho e mais usuários passaram a utilizá-los em seu dia a dia, em conjunto com os mainframes. A necessidade de segurança aumenta pois também temos que proteger os dados e informações presentes nas máquinas dos usuários

- Os computadores começaram a se comunicar entre si e compartilhar informação em tempo real graças às redes e a internet, os servidores diminuíram, e o cenário de segurança ficou mais crítico, já que a informação tem que estar sempre disponível, mas também segura (confidencialidade, integridade). Aqui começaram também as transações financeiras pelos computadores.

- Finalmente, nos dias de hoje, além de tudo isso temos as ferramentas de comunicação em massa e as redes sociais, que são um grande problema para o pessoal de segurança da informação.
- Além disso, os equipamentos de informática estão cada vez mais baratos e todo mundo tem acesso a tecnologia (smartphones, tablets, notebooks, etc.)
- Hoje em dia é difícil ver uma empresa que não tenha uma pequena rede e que faça suas transações usando os recursos da informática, e com isso a área de segurança ganha maior importância.



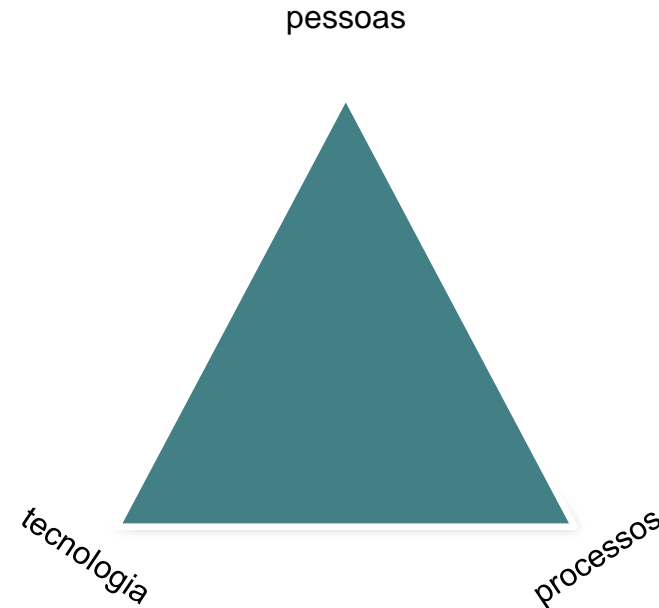
# MAIOR DIFICULDADE NA ADOÇÃO DE PROCEDIMENTOS DE SEGURANÇA

- Quando implantamos procedimentos de segurança nas empresas sempre temos que restringir acessos e implementar algumas proibições.
- Isso gera as mais diversas reações nos usuários.
- Existem aqueles que aceitam as imposições necessárias mas a maioria não gosta e fica contra, pois isso afeta sua liberdade.



- Mas por que os usuários tem tanta resistência aos procedimentos de segurança?
  - Pessoas não gostam de sofrer restrições
  - Pessoas não gostam de seguir regras
  - Pessoas não gostam de esperar aprovações
  - Pessoas não gostam de decorar senhas
  - Pessoas não gostam de mudanças
- Por isso, os profissionais de segurança encontram grande dificuldade em implementar os controles necessários.
- Além disso, ainda temos que alinhar as necessidades de segurança com as necessidades empresariais do negócio.

- Segurança envolve 3 aspectos:



- Pessoas: todo capital humano
- Processos: normas e procedimentos
- Tecnologia: hardware, software e redes

**DESSES, QUAL O PONTO MAIS PROBLEMÁTICO??**

- Pensar em segurança sempre envolve pensar em 3 fatores:
  - O que proteger.
  - Como proteger.
  - De que (ou de quem) proteger.

# CIDAL

- Muitas empresas pensam e adotam estratégias para a Segurança de suas Informações, porém, numa amplitude limitada.
- A segurança vai muito além dos acessos via "usuário e senha" para esse ou aquele usuário, ou da instalação do antivírus.

- A melhor maneira de se pensar em Segurança das Informações é seguir algumas diretrizes consagradas no mercado.
- Essas diretrizes cobrem a totalidade das providências que devem ser adotadas, a fim de que as informações das empresas passem por todo seu ciclo de vida sob a melhor maneira de estarem seguras.

- Sempre que pensamos em segurança, temos de ter em mente que precisamos garantir alguns pilares básicos. Esses pilares básicos são conhecidos como CIDAL:

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Legalidade

# SEGURANÇA

C  
O  
N  
F  
I  
D  
E  
C  
I  
A  
L  
I  
D  
A  
D  
E

I  
N  
T  
E  
G  
R  
I  
D  
A  
D  
E

D  
I  
S  
P  
O  
N  
I  
B  
I  
L  
I  
D  
A  
D  
E

A  
U  
T  
E  
N  
T  
I  
C  
I  
D  
A  
D  
E

L  
E  
G  
A  
L  
I  
D  
A  
D  
E

# Confidencialidade

- Garantir que a informação só pode ser acessada por pessoas autorizadas.
- É um assunto de alta importância nas empresas.
- A confidencialidade vai de encontro com o acesso físico e lógico da empresa.
- A definição de "quem pode" e "até onde pode" acessar carece de muita análise e discussões entre todos os envolvidos.
- Manter as informações sob a confidencialidade é adotar meios que garantam que as informações sejam acessadas somente por aqueles que tem permissão de acessá-las.



- Não existe uma fórmula ou regra a ser seguida. As empresas são diferentes e as deliberações de permissões também para cada uma.
- O importante é ter a diretriz da confidencialidade atendida, sempre!

# Integridade

- Garantir que as informações não sofram quaisquer alterações desde seu envio até o armazenamento, incluindo-se aqui seu transporte. A ideia é proteger as informações contra alterações indevidas (intencionais ou não).
- De nada servem informações não confiáveis para as empresas.
- Toda informação deve tratada como um "precioso bem" para a empresa. Dessa forma, a empresa deve prover meios que garantam que todas suas informações sejam criadas com integridade e manipuladas sob a mesma diretriz.

- Para isso, alguns processos precisam ser observados.
  - Quem pode acessar a informação
  - Registro de quem acessou ou alterou a informação
  - Autorizações de alterações e registro das autorizações
  - Monitoramento constante dos sistemas
- A integridade zela para que haja processos, previamente definidos, para toda e qualquer manipulação de informações na empresa.
- Esses processos devem seguir permissões e, se for o caso, passarem por autorizações além de prever o registro das alterações e das autorizações para eventuais auditorias.

# Disponibilidade

- Garantir que as informações estarão sempre disponíveis para que as pessoas autorizadas possam acessar as mesmas quando necessitarem fazer uso da mesma para a execução de suas tarefas diárias.

- Hoje, as empresas estão cada vez mais informatizadas e dependentes de suas informações.
- Porém não basta possuir as informações somente, elas devem ser íntegras e estarem disponíveis sempre que necessárias para uso das pessoas com autorização.
- A disponibilidade orienta para que a empresa defina processos a fim de que seja garantido o fornecimento de informações quando necessárias.
- **Lembrem-se: Informações são importantíssimas e estratégicas!**

- São baseadas nelas que as diretorias das empresas desenvolvem seus planos, estratégias de negócio, desenvolvem novos produtos, avaliam mercados, etc.
- Dessa maneira, a TI atualmente lida com a "alta disponibilidade", ou seja, garante que as informações possam ser acessadas em quase 100% do tempo. Exceções são feitas aos períodos de manutenção nas bases de dados ("janelas de processamento").

# Autenticidade

- Garantir que os usuários que estão acessando e usando as informações são eles mesmos. Devemos validar os usuários que acessam a informação garantindo que o usuário não poderá negar um acesso depois que ele o efetuar.
- Trata-se de uma diretriz de suma importância, pois orienta a empresa para que providencie processos que garantam que a pessoa ou sistema que está acessando a informação, realmente seja quem diz ser e, realmente, está autorizado a acessá-la.

- A autenticidade se relaciona com confidencialidade, integridade e disponibilidade...
- Para garantir a autenticidade, alguns métodos podem ser implementados, como:
  - Usuário e senha.
  - Biometria.
  - Criptografia.



# Legalidade

- Garantir o cumprimento das leis vigentes (federais, estaduais ou municipais) e as normas internas da empresa, zelando para que a forma como a empresa lida com as informações estejam de acordo com essas leis.
- É um grande desafio, pois pessoas habilitadas para acesso às informações nem sempre agem de maneira profissional, mas para obterem vantagens pessoais e financeiras e, aliado ao fato da ausência de mecanismos legais punitivos, gera-se com isso um ambiente vulnerável às fraudes.

- É fundamental que situações ainda não previstas em lei sejam adequadamente tratadas em códigos de ética corporativos.
- Com o envolvimento de seres humanos, fica praticamente impossível que seja garantida a segurança das informações em 100% do tempo.
- Não há seres humanos 100% confiáveis em 100% do tempo.
- As empresas devem adotar meios para que suas vulnerabilidades sejam mitigadas.
- O CIDAL é um excelente direcionamento a ser seguido.

# Ciclo de Vida da Informação

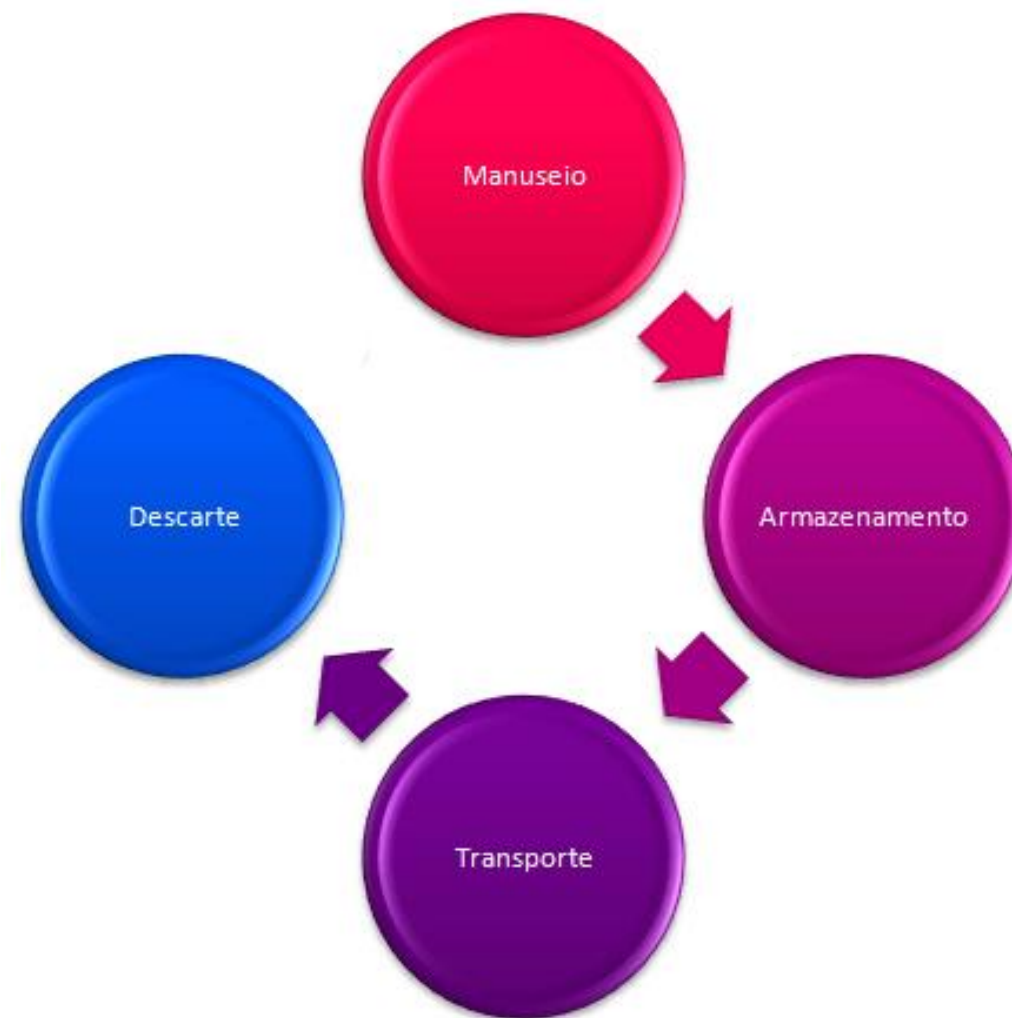
- Dentro da empresa, a informação passa por diversas etapas, e precisamos conhecer cada uma delas para protegê-la de maneira adequada.
- Cada momento deve ter seus controles e preocupações específicos.

**O ciclo de vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa. (Sêmola, 2003)**

- O ciclo de vida são as etapas pelas quais a informação passa, desde quando ela é criada até o momento em que ela não tem mais utilidade.
- Em geral, o ciclo de vida engloba:
  - **MANUSEIO** - momento em que a informação é criada ou manipulada).
  - **ARMAZENAMENTO** - momento em que a informação é salva;
  - **TRANSPORTE** - momento em que a informação é enviada;
  - **DESCARTE** - momento em que a informação é apagada.

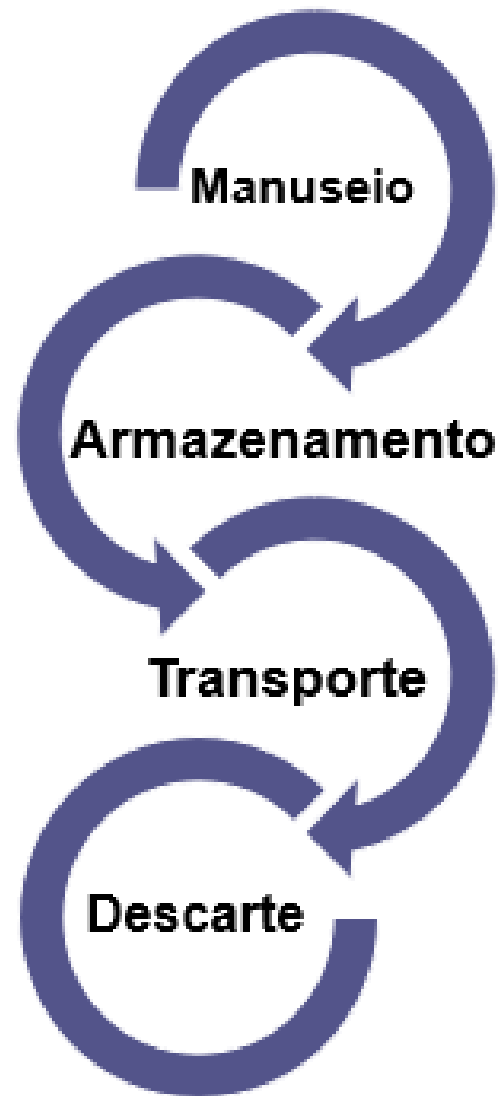
1. **Manuseio:** quando, como e onde a informação é criada ou manipulada. É uma etapa que pode ocorrer diversas vezes durante o ciclo de vida da informação. Ex: gráficos de despesas são gerados pelo departamento financeiro todo dia 30 usando a ferramenta MS Excel.
2. **Armazenamento:** como e onde a informação é gravada. A informação pode ser armazenada em meio físico ou lógico. Essa etapa sempre ocorre quando uma informação é criada ou alterada. Ex: o gráfico de despesas deve ser salvo no servidor XXX, na pasta YYY.

3. **Transporte:** quando a informação é transmitida, deixa seu local original. Quando a informação sai de um local e vai para outro. Ex: o gráfico de despesas só pode ser enviado pelo e-mail corporativo.
4. **Descarte:** quando a informação é completamente eliminada. Quando o uso da informação é encerrado, quando ela não é mais necessária de maneira alguma. Ex: apagar do servidor e dos itens enviados e destruir os impressos que foram gerados.





## Ciclo de Vida da Informação



## CIDAL

### Segurança da Informação

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Legalidade

# Para reflexão...



# Para saber mais...

## Vídeos:

O que é Segurança da Informação Digital

[https://www.youtube.com/watch?v=WDqiQzzE\\_30](https://www.youtube.com/watch?v=WDqiQzzE_30)

Navegar é preciso

<https://www.youtube.com/watch?v=QyOhW-cOpT0&list=PLA36AA58B0285BB12>

Segurança da Informação

<https://www.youtube.com/watch?v=ZD66EMgB1FA&t=363s>