

# Princípios da Segurança e o Ciclo de Vida da Informação



# Princípios da Segurança e o Ciclo de Vida da Informação

- Unidade 1-Princípios da segurança e o ciclo de vida da informação
- 1.1- O que visa a segurança da informação
- 1.2- Valor da Informação
- 1.3- Integridade, Confidencialidade e Disponibilidade
- 1.4- Autenticidade e não repúdio(Irretratabilidade)
- 1.5- Sistemas de autenticação
- 1.6- Segurança Física e Lógica
- 1.7- Controle de Acesso Físico e Lógico
- 1.8- Ciclo de vida da informação

# 1.1 O que visa a Segurança da Informação

- A Segurança da Informação (SI) está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: Confidencialidade, Integridade, Disponibilidade e Autenticidade.



# 1.1 O que visa a Segurança da Informação

- A SI não está restrita somente a Sistemas Computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados.



# 1.1 O que visa a segurança da informação

- A maioria das definições de Segurança da Informação (SI) pode ser resumizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas.
- A SI não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma.
- É importante lembrar que a SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

# 1.1 O que visa a segurança da informação

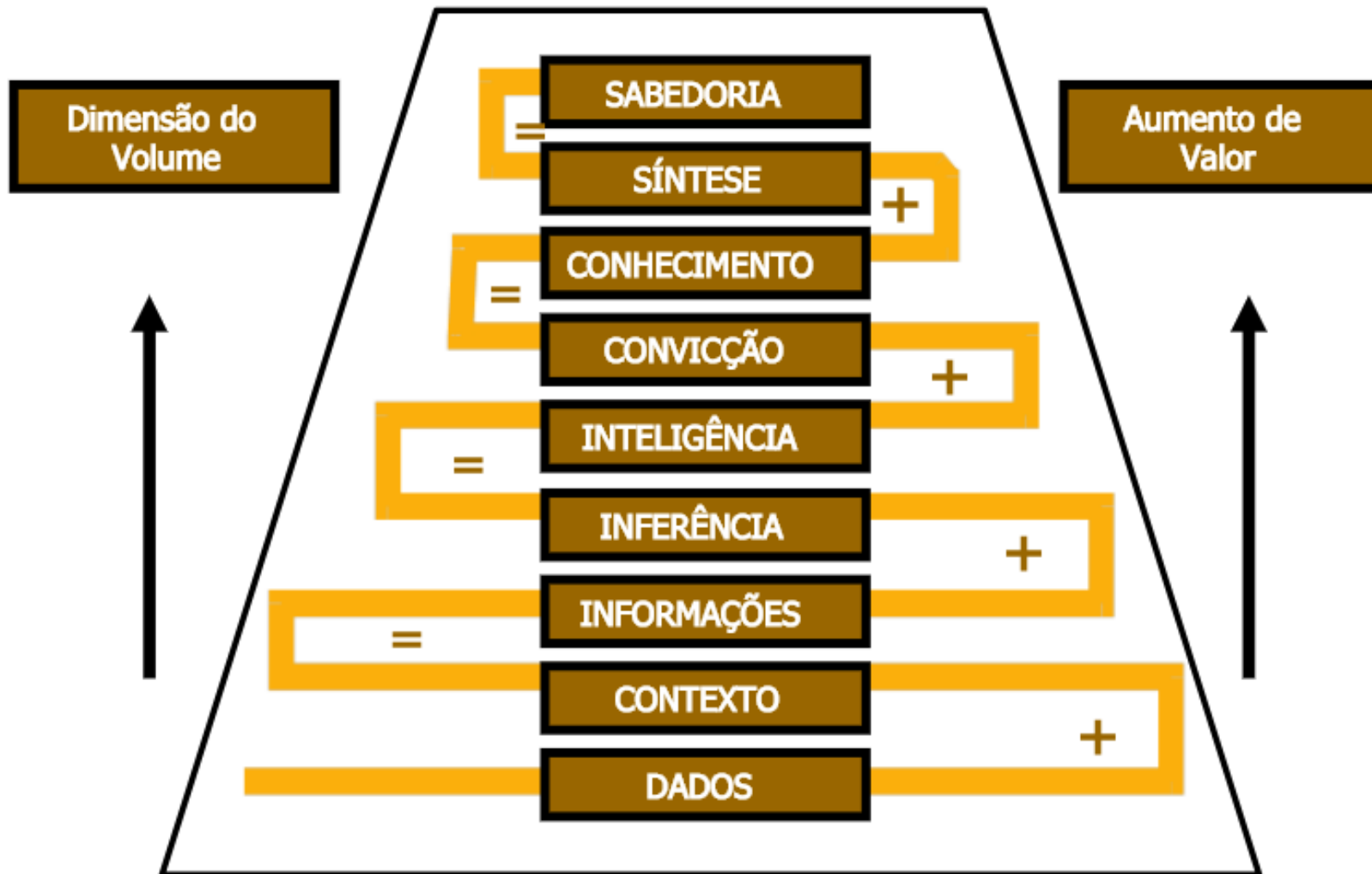
- A Segurança da informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais.
- Entende-se por Informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

# 1.1 O que visa a segurança da informação

- Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente.
- A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

# 1.2 Valor da Informação


## Valor da Informação








# 1.2 Valor da Informação

## Definições sobre Informação

**Dados**  Qualquer elemento (aspecto, fato, medida etc.) representativo, disponível e coletável na realidade; "fatos no estado bruto", conforme Platão;

Qualquer construção derivada da composição de dados, que seja significativa no reconhecimento, compreensão e/ou modelagem da realidade;  **Informação**

**Inteligência**  Apreensão, compreensão, adaptação e/ou percepção da realidade, suportada por processamento de informação;

Conjunto de conceitos, noções, idéias, mecanismos e conexões/associações, utilizado na abordagem da realidade, definido e construído a partir dos produtos gerados pela inteligência.  **Conhecimento**

## 1.2 Valor da Informação

- Informação é um bem valioso que pode ajudar ou quebrar a sua empresa.
- Quando gerenciada corretamente ela lhe permite operar com confiança.
- Gestão de segurança da informação lhe dá a liberdade de crescer, inovar e ampliar sua carteira de consumidores, sabendo que todas as suas informações confidenciais permanecerão assim.

## 1.2 Valor da Informação

- Com o desenvolvimento tecnológico e a necessidade da empresa buscar o crescimento constantemente, onde o foco é a busca incessante pela informação, a organização passou a ter a internet ou as redes de computadores como seu maior aliado para a sobrevivência neste mercado competitivo.
- Com o auge da competitividade, a informação passou a ter um valor maior representando assim benefícios para a organização.

## 1.2 Valor da Informação

- A informação é um bem que tem alto valor para a empresa, mas este bem só poderá ser utilizado se for devidamente protegido. A informação protegida proporciona a organização tomar decisões precisas para os seus negócios.
- Atualmente, com a grande concorrência existente no mercado, mais do que nunca o mercado totalmente globalizado é necessário ter uma informação sempre mantida em sigilo nos meios empresariais.

## 1.2 Valor da Informação

- Cada empresa mantém sua informação como um meio de ganhar ou somar pontos perante a uma concorrência que o mercado às impõe.
- Esta informação, que é um conhecimento que a organização adquire através de um processamento de um conjunto de dados, também é a principal ferramenta adquirida que dispõem de um grande valor de mercado.

## 1.2 Valor da Informação

- No passado, antes do advento tecnológico, as informações ficavam guardadas de várias formas: impressas ou escritas em papel, em mente com o próprio proprietário ou com pessoas de confiança e, na maioria das vezes, guardadas como um amontoado de papéis arquivados em grandes armários.
- Hoje esta informação necessita ser armazenada e tratada de maneiras diferentes.
- No entanto, podemos dizer que a maneira mais adequada para uma empresa em termos de armazenamento é o uso do meio digital.

## 1.2 Valor da Informação

- Na verdade, a tecnologia deste tipo de dispositivo evolui a cada dia, possibilitando a gravação de uma alta carga de informações em menores estruturas ou na Nuvem.
- Fato este é o grande volume de informações trabalhadas no dia a dia, ao valor que ela tem para mercado e as constantes mudanças que sofrem.

## 1.2 Valor da Informação

- Com toda essa importância, a vasta quantidade de informação fez com que as empresas se tornassem mais dependentes do processo tecnológico, buscando na informática a dependência de diversos serviços.
- Essa corrida para cumprir as necessidades fez com que as preocupações e os devidos cuidados com uma estrutura de segurança não fossem seguidos, visto que a vulnerabilidade, o desconhecimento ou a má prática de normas de segurança ainda estão presentes nos dias atuais.



## 1.2 Valor da Informação

- Portanto, para manter essa proteção é necessário que medidas de segurança sejam tomadas.
- Os procedimentos, regras ou normas realmente precisam ser utilizados por todos que atuam na organização, independente de que cargo exerce na empresa. Com isso, o resultado final será o ganho da organização em manter suas atividades e negócios bem sucedidos.
- Não podemos considerar a informação como um produto final, mas sim, o ponto de partida que leva a um processo de tomada de decisão.

# 1.3 Integridade, Confidencialidade e Disponibilidade



## Confidencialidade

- Assegurar que a informação é acessível somente por aqueles devidamente autorizados

## Integridade

- Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento

## Disponibilidade

- Assegurar que quem devidamente autorizado tem acesso á informação e bens associados sempre que necessário

# 1.3 Integridade, Confidencialidade e Disponibilidade

- Portanto os atributos básicos da **segurança da informação**, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:
- Confidencialidade: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida;
- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- 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 ou Não-Repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita;
- Conformidade: propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

## 1.4 Autenticidade e não repúdio (Irretratabilidade)

- A tríade CIA (*Confidentiality, Integrity and Availability*) Confidencialidade, Integridade e Disponibilidade — representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger.
- Outros atributos importantes são não-repúdio (irretratabilidade), autenticidade e conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação. Aí vem a Lei 13.709 de 14/08/2018.

# Adendo: Lei 13.709

- Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- *Este tema será abordado com mais profundidade posteriormente.*

## 1.4 Autenticidade e não repúdio (Irretratabilidade)

- 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 ou Não Repúdio: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.



## 1.5 Sistemas de Autenticação

- Em Segurança da Informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema no momento em que ele requisita um login (acesso) em um programa ou computador/rede, ou seja, suas credenciais de acesso.



# 1.5 Modos de Autenticação

- A autenticação, em regra, depende de um ou mais modos ou fatores:
  - Algo que o usuário é: geralmente são usados meios biométricos, como impressão digital, padrão de retina, padrão de voz, reconhecimento de assinatura, reconhecimento facial.
  - Algo que o usuário tem: usa-se objetos específicos como cartões de identificação, smart cards, tokens USB.
  - Algo que o usuário conhece: são utilizadas senhas fixas, on time passwords, sistemas de desafio-resposta.
  - Onde o usuário está: quando o acesso a sistemas só pode ser realizado em uma máquina específica, cujo acesso é restrito.

## 1.5 Modos de Autenticação: Senha

- Senhas são utilizadas no processo de verificação da identidade do usuário (login), assegurando que este é realmente quem diz ser.

## 1.5 Modos de Autenticação: Senha

- Para garantir uma boa segurança às senhas utilizadas, são definidas algumas regras básicas:
  - Jamais utilizar palavras que façam parte de dicionários, nem utilizar informações pessoais sobre o usuário (data de nascimento, parte do nome, etc.).
  - Uma boa senha deve ter pelo menos oito caracteres, de preferência com letras, números e símbolos.
  - A senha deve ser simples de digitar e fácil de lembrar.
  - Usar uma senha diferente para cada sistema utilizado.
  - Tentar misturar letras maiúsculas, minúsculas, números e sinais de pontuação.
  - Trocar as senhas a cada dois ou três meses, e sempre que houver desconfiança que alguém descobriu a senha.

## 1.5 Modos de Autenticação: Senha

- No ambiente corporativo, deve haver outros cuidados para a proteção do sigilo da senha, como:
  - Se certificar de não estar sendo observado ao digitar a sua senha;
  - Não fornecer sua senha para qualquer pessoa, em hipótese alguma;
  - Não utilize computadores de terceiros (por exemplo, em LAN houses, cybercafés, etc) em operações que necessitem utilizar suas senhas;
  - Se certificar de que seu provedor disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

## 1.5 Modos de Autenticação: Senha

- No caso do usuário Administrador (ou root), devem ser tomados alguns cuidados especiais, uma vez que ele detém todos os privilégios em um computador:
  - Utilizar o usuário Administrador apenas quando for necessário, ou seja, para realizar comandos que os usuários comuns não sejam capazes de fazer;
  - Elaborar uma senha para o usuário Administrator, com uma segurança maior que a exigida pelo usuário comum;
  - Criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador, para substituir o uso do usuário Administrator em tarefas rotineiras.

## 1.5 Modos de Autenticação: On-Time Password

- One-time passwords são senhas de uso único. A senha a ser utilizada pode ser definida de acordo com o horário ou a quantidade de acessos, de forma que não seja possível a reutilização de uma senha. Esse sistema garante maior segurança, e é usado em sistemas de alta criticidade, como transações bancárias. Entretanto, o problema desse sistema é a dificuldade de administração, uma vez que é preciso o uso de ferramentas adicionais para guardar as senhas, como, por exemplo, tokens de segurança usados por bancos (Token OTP).

### *Tokens*

*A palavra significa “passe” e remete aos dispositivos geradores de códigos aleatórios, necessários para acessar sua conta bancária juntamente com a senha individual. Desta forma, ninguém poderá adivinhar o código, já que ele é gerado instantaneamente.*



# 1.5 Modos de Autenticação: Smart Cards

- Smart Cards são cartões que possuem um microchip embutido para o armazenamento e processamento de informações. Ele pode ser programado e, geralmente, é usado para guardar informações sobre o usuário. O acesso às informações, geralmente, é feito por meio de uma senha (Código PIN) e há um número limitado de tentativas de acesso sem sucesso. Caso estoure esse limite, o cartão é bloqueado, e só é reativado por meio de um outro código (Código PUK), que também tem um número limitado de tentativas de acesso. Caso estoure esse outro limite, o cartão é inutilizado.



## 1.6 Segurança Física e Lógica

- Segurança física é a forma de proteger equipamentos e informações contra usuários que não possuem autorização para acessá-los.
- Enquanto segurança lógica é um conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou programas desconhecidos.
- As duas formas de proteção são essenciais para lidar com as ameaças à informação. Por isso é importante conhecer como cada uma delas é executada e como melhorá-las.



## 1.6 Segurança Física

- A segurança física é feita nas imediações da empresa e leva em consideração a prevenção de danos causados por desastres locais ou ambientais, como terremotos, inundações e incêndios. Por isso, investigar a ocorrência de eventos climáticos passados é importante ao se planejar os métodos de segurança física para proteção de funcionários, equipamentos, dados e do local.
- Além disso, ela trata de métodos para evitar o acesso de pessoas não autorizadas a áreas em que se encontram dados e informações críticas da empresa. Uma forma de fazer isso é implantar recursos de identificação de funcionários, como o uso de crachás, senhas e cadastro de digitais.

## 1.6 Segurança Física

- Para ter uma boa segurança física é importante controlar a entrada e saída de equipamentos, materiais e pessoas da empresa por meio de registros de data, horário e responsável.
- Quando há a entrada de visitantes na empresa, eles não devem andar sozinhos, o ideal é que sejam acompanhados por algum funcionário até o local de destino e registrados no sistema.

## 1.6 Segurança Física

- Outro tipo de reforço para a segurança local é usar mecanismos, como fechaduras eletrônicas, câmeras e alarmes, para controlarem o acesso aos ambientes que guardam backups e computadores com dados confidenciais.
- Para desenvolver uma boa segurança física é preciso analisar qual é o perfil da empresa, o tipo de proteção necessária, os investimentos possíveis e definir uma política de controle de acesso físico que se encaixe ao modelo de negócio.

## 1.6 Segurança Lógica

- Esse tipo de proteção controla o acesso a aplicativos, dados, sistemas operacionais, senhas e arquivos de log por meio de firewalls de hardwares e softwares, criptografia, antivírus e outras aplicações contra hackers e possíveis invasões às fontes internas da empresa.
- A segurança lógica permite que o acesso seja baseado nas necessidades específicas de cada usuário para realizar suas tarefas, fazendo a identificação por meio de senha e login.
- Assim, nenhum funcionário poderá executar funções que não sejam de seu cargo.
- Para aprimorar esses mecanismos, é importante sempre manter sistemas e protocolos operacionais atualizados.

## 1.6 Segurança Lógica

- A proteção da informação vem sendo um grande desafio para as empresas, devido às diversas ameaças existentes que podem trazer grandes prejuízos.
- Por isso, para se ter uma proteção eficaz dos dados, é importante ter uma equipe de TI bem treinada e atualizada com as novas tecnologias de segurança da informação que surgem a cada dia e encontram novas soluções de segurança.
- Os riscos que uma empresa corre por não ter uma boa estrutura de segurança lógica são muitos, como acesso de terceiros a informações sigilosas, perdas de dados, falhas na rede causada por fraudes, entre outros.

## 1.6 Segurança Lógica

- Os principais riscos à segurança da informação são: a perda de confidencialidade, que acontece quando há quebra de sigilo e informações restritas apenas a determinados funcionários são vazadas; a perda de integridade, que significa que uma pessoa não autorizada consegue ter acesso e modificar algum dado importante e a perda de disponibilidade, quando pessoas autorizadas passam a não conseguir acessar uma aplicação que necessitam.

## 1.6 Segurança Lógica

- Os principais riscos à segurança da informação são: a perda de confidencialidade, que acontece quando há quebra de sigilo e informações restritas apenas a determinados funcionários são vazadas; a perda de integridade, que significa que uma pessoa não autorizada consegue ter acesso e modificar algum dado importante e a perda de disponibilidade, quando pessoas autorizadas passam a não conseguir acessar uma aplicação que necessitam.

## 1.7 Controle de Acesso

- Controle de acesso é o processo de autorizar usuários, grupos e computadores a acessarem objetos na rede.
- Os principais conceitos que compõem o controle de acesso são as permissões, os direitos do usuário e a auditoria de objetos.







## 1.7 Permissões

- As permissões definem o tipo de acesso concedido a um usuário ou grupo para um objeto ou propriedade de objeto.
- As permissões são aplicadas a quaisquer objetos seguros, como arquivos, objetos do Active Directory® ou objetos do Registro. Pode-se conceder permissões a qualquer usuário, grupo ou computador. Atribuí-las a grupos é uma boa prática.
- Você pode atribuir permissões aos objetos para:
  - Grupos, usuários e Identificadores de Segurança no domínio.
  - Grupos e usuários desse domínio e de domínios confiáveis.
  - Grupos e usuários locais do computador no qual o objeto reside.



## 1.7 Permissões

- As permissões anexadas a um objeto dependem do tipo do objeto. Por exemplo, as permissões que podem ser anexadas a um arquivo diferem das que podem ser anexadas a uma chave do Registro. Algumas permissões, no entanto, são comuns à maioria dos tipos de objetos. Essas permissões são:
  - Permissões de leitura
  - Modificar permissões
  - Alterar proprietário
  - Excluir

## 1.7 Permissões

- Ao configurar permissões, você especifica o nível de acesso para grupos e usuários. Por exemplo, você pode deixar um usuário ler o conteúdo de um arquivo, deixar outro usuário fazer alterações no arquivo e evitar que todos os outros usuários acessem o arquivo. É possível definir permissões similares em impressoras, para que determinados usuários possam configurar a impressora e outros usuários possam apenas imprimir nela.
- Se você precisar alterar as permissões em um objeto individual, poderá iniciar a ferramenta apropriada e alterar as propriedades do objeto. Por exemplo, para alterar as permissões em um arquivo, você pode iniciar o Windows Explorer, clicar com o botão direito do mouse no nome do arquivo e clicar em **Propriedades**. Na guia **Segurança**, você pode alterar as permissões no arquivo.

## 1.7 Informações Físicas e Digitais

- Pesquisadores da área de tecnologia da informação advertem para o fato de que sistemas de informação computadorizados são mais vulneráveis a destruição, erros, mau uso e crime do que os sistemas manuais, em que a informação é geralmente guardada sob a forma de registros em papel.
- Algumas formas possíveis de agregar segurança aos sistemas de informação computadorizados são instalação de sistemas de segurança de acesso, tais como login e senhas e instalar sistemas de proteção contra vírus e hackers.

## 1.7 Propriedade de Objetos

- Quando o objeto é criado, um proprietário é atribuído a ele. Por padrão, o proprietário é o criador do objeto.
- Independentemente das permissões definidas para um objeto, o seu proprietário sempre poderá alterá-las.

### Atributos

Dono	Grupo	Público
<input checked="" type="checkbox"/> Ler	<input checked="" type="checkbox"/> Ler	<input checked="" type="checkbox"/> Ler
<input checked="" type="checkbox"/> Escrever	<input type="checkbox"/> Escrever	<input type="checkbox"/> Escrever
<input checked="" type="checkbox"/> Executar	<input checked="" type="checkbox"/> Executar	<input checked="" type="checkbox"/> Executar
7	5	5

Alterar Permissões

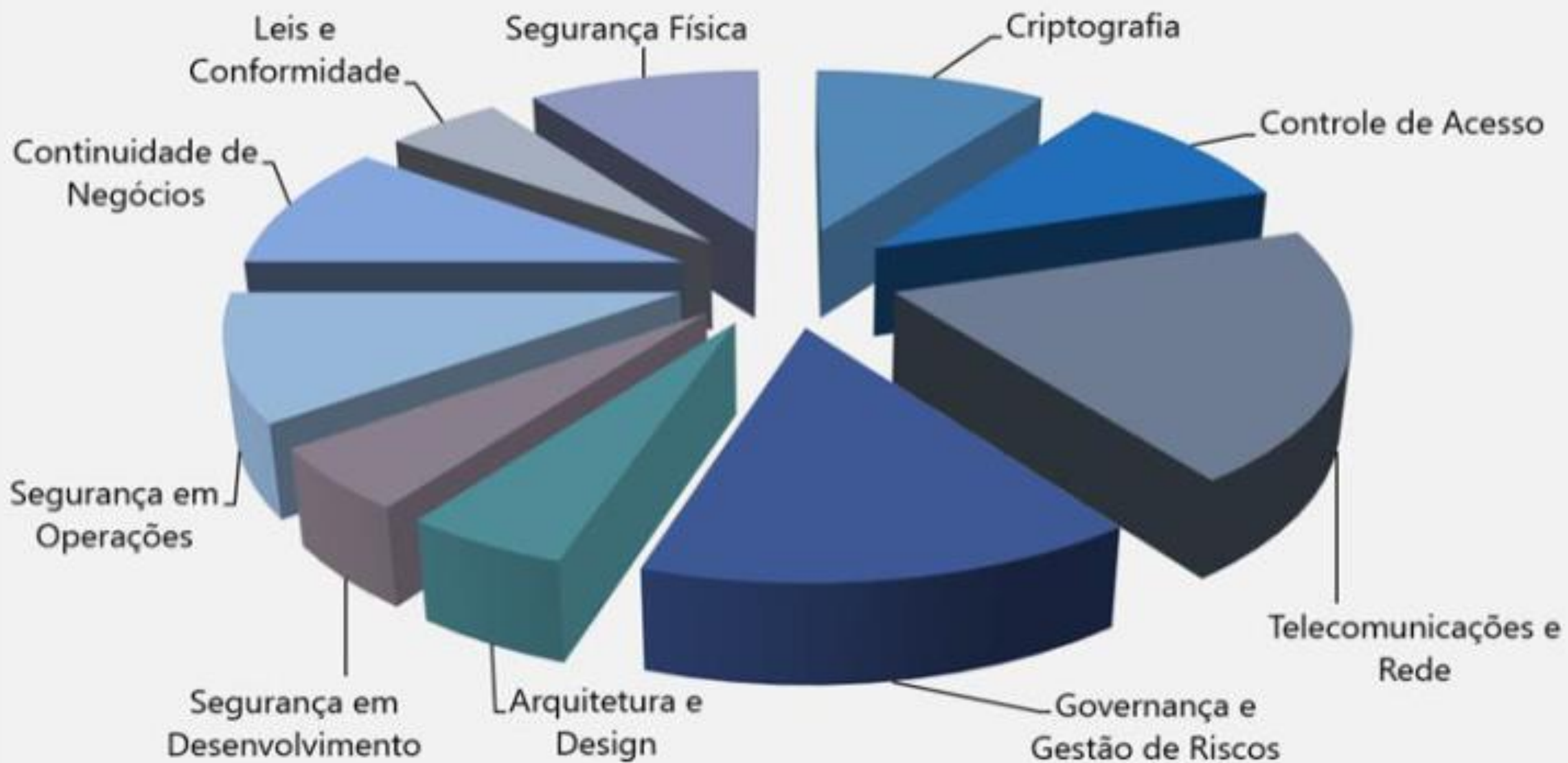


## 1.7 Herança de Permissões

- A herança permite que os administradores atribuam e gerenciam permissões com facilidade.
- Esse recurso faz com que os objetos contidos em um recipiente herdem automaticamente as permissões desse recipiente.
- Por exemplo, os arquivos contidos em uma pasta, quando criados, herdam as permissões da pasta.
- Somente as permissões marcadas para serem herdadas serão herdadas.



# Domínios da Segurança da Informação



## 1.7 Direitos do Usuário

- Os direitos do usuário concedem privilégios e direitos de logon específicos a usuários e grupos em seu ambiente de computação.

## 1.7 Auditoria de Objetos

- Você pode auditar o acesso dos usuários a objetos. Você poderá exibir os eventos relacionados à segurança no log de segurança com o recurso.







## 1.7 Segurança - Permissões e Descritores

- Todo recipiente e objeto da rede possui um conjunto de informações sobre o controle de acesso anexado a ele. Denominadas descritores de segurança, essas informações controlam o tipo de acesso permitido a usuários e grupos. O descritor de segurança é criado automaticamente junto com o recipiente ou objeto. Um arquivo é um exemplo comum de um objeto com um descritor de segurança.
- As permissões são definidas em um descritor de segurança do objeto. Elas são associadas a usuários e grupos específicos, ou a eles atribuídas. Por exemplo, para o arquivo Temp.dat, é possível atribuir as permissões de leitura, gravação e exclusão ao grupo **Administrador**, enquanto o grupo **Operador** pode receber apenas permissões de leitura e gravação.

## 1.7 Segurança ao Acesso

- Na segurança eletrônica, o controle de acesso desempenha um papel importante para identificar as pessoas presentes em uma determinada área controlada. O Controle de acesso de pessoas em áreas restritas, principalmente DataCenters, entre outros, é feito através de equipamentos como portas eletrônicas, catracas, torniquetes e cancelas. Todos os acessos são registrados em um software e banco de dados desenvolvidos para este fim. Com isto é possível rastrear todas as pessoas que estão, ou estiveram presentes na área controlada. Para autenticar e autorizar uma pessoa são utilizadas diversas tecnologias como: cartão de proximidade, biometria e senha.





Controle de Cargas

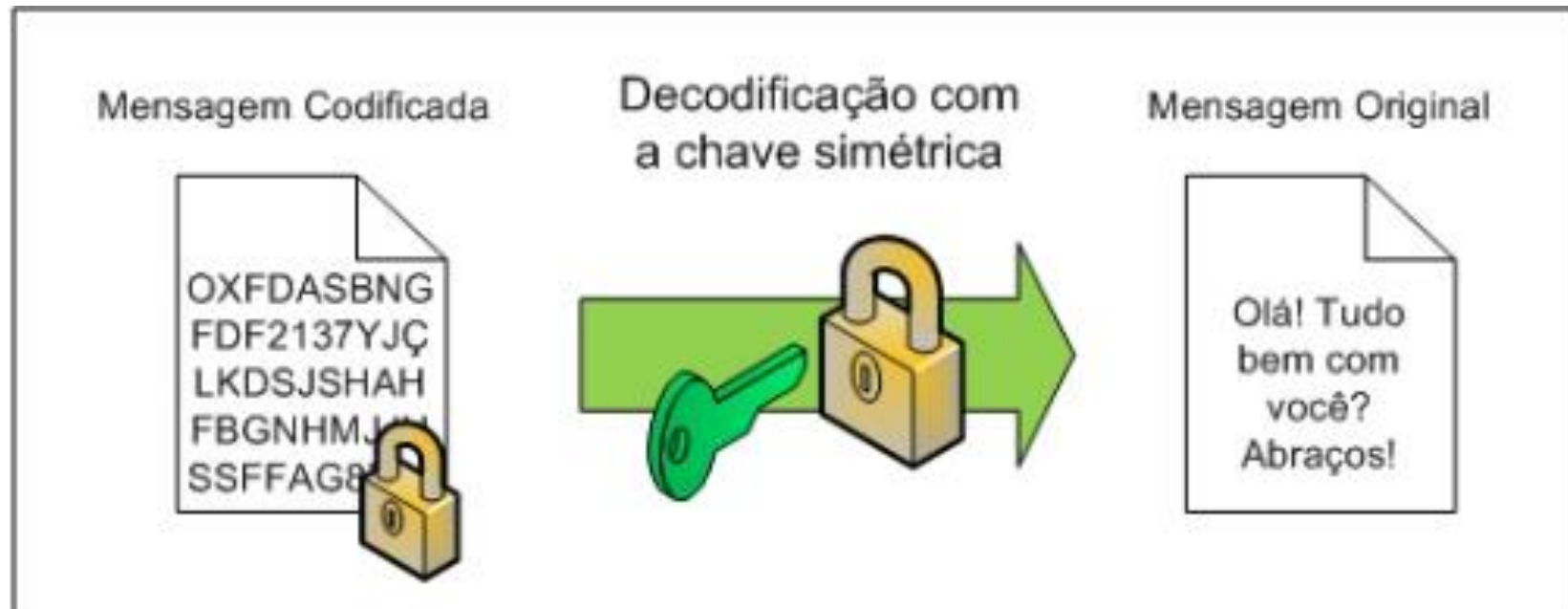


Controle de Acesso



# 1.7 Criptografia

- **Criptografia** (do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

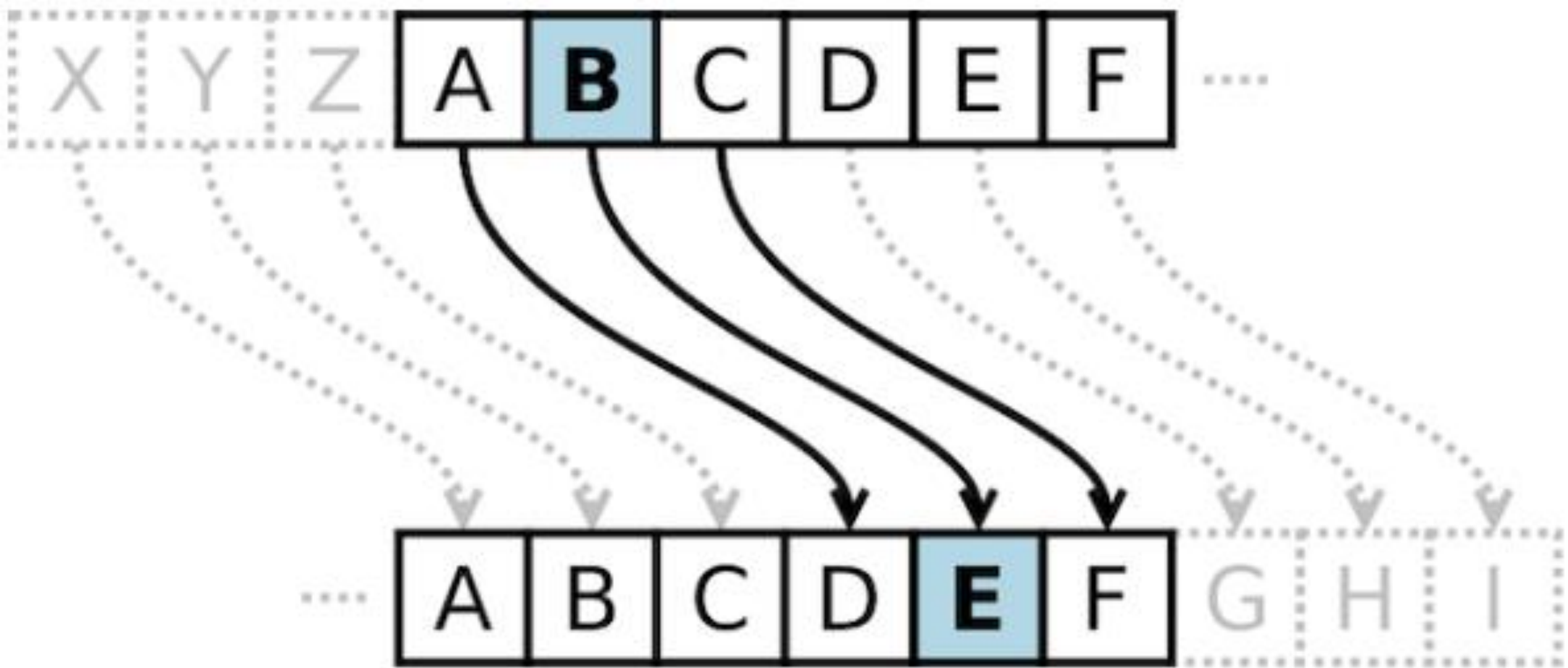




## 1.7 Criptografia

A criptografia tem quatro objetivos principais:

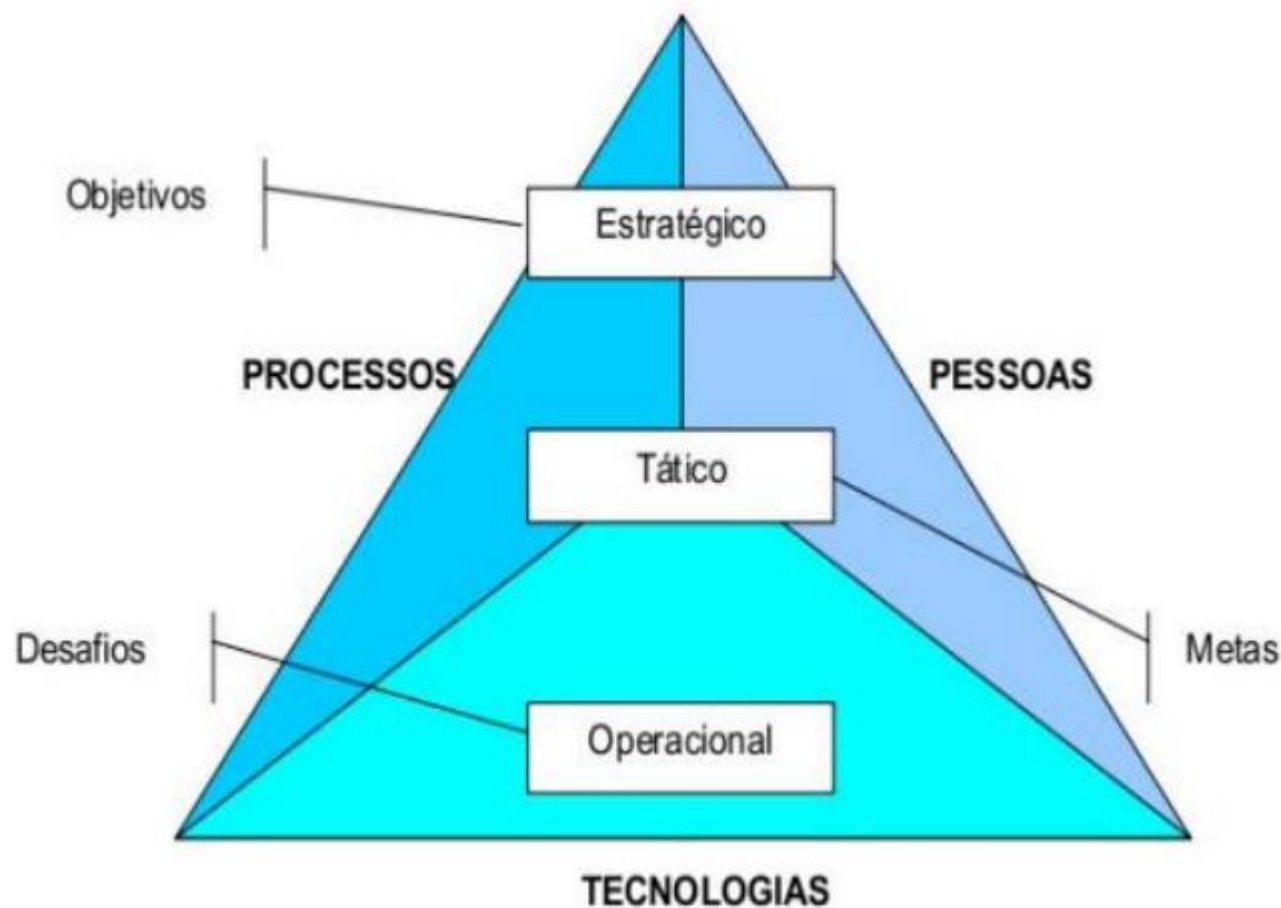
- **confidencialidade** da mensagem: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.
- **integridade** da mensagem: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.
- **autenticação** do remetente: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.
- **não-repúdio** ou **irretratabilidade** do emissor: não deverá ser possível ao emissor negar a autoria da mensagem.



## 1.8 Ciclo de Vida da Informação

- Toda informação possui um ciclo de vida.
- Um dado é gerado, permanece disponível pelo tempo necessário, passa por atualizações e, depois, ao perder sua serventia, deve ser descartado adequadamente.

## 1.8 Ciclo de Vida da Informação



Pirâmide Estratégica da Informação

## 1.8 Ciclo de Vida da Informação

- **Manuseio:** Refere-se ao instante em que a informação é criada e/ou passa a ser manipulada;
- **Armazenamento:** Como e onde armazenar determinados tipos de informações;
- **Transporte:** Abrange todo o tipo de transporte possível para uma informação(e-mail, entrega via transportadora, mensageria, etc.)
- **Descarte:** Procedimentos a serem adotados no momento da exclusão de uma informação e quando o descarte deve ocorrer.