

# **AULA 09**

# **SISTEMAS DE INFORMAÇÃO**

**Segurança em Sistemas  
de Informação**

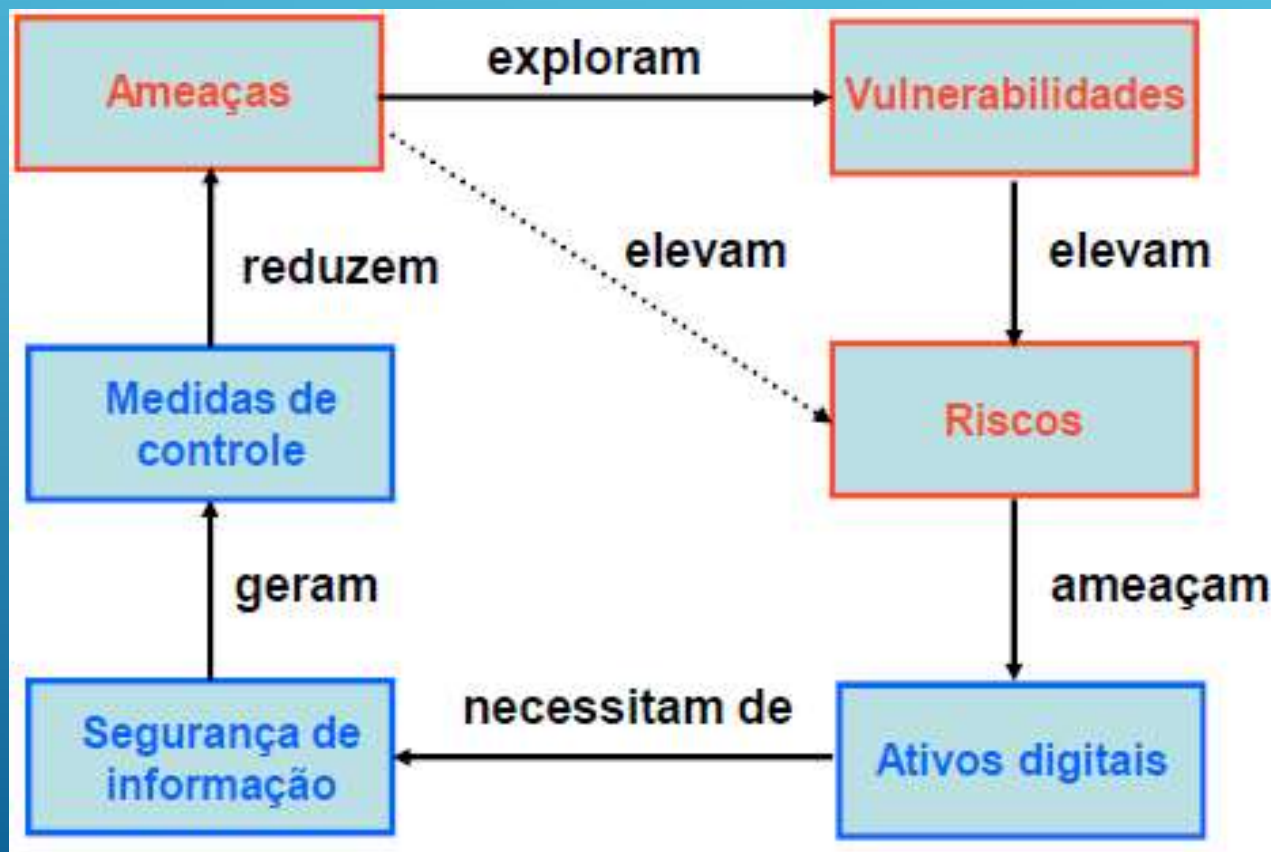
# OBJETIVOS

- Entender a importância da proteção das informações do clientes e da empresa e a necessidade da proteção sobre dados que possuem valor para alguém ou para uma organização.
- Conhecer os aspectos básicos de confidencialidade, integridade e disponibilidade da informação e compreender necessidades de sua proteção.

# SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

**Objetiva a proteção** das **informações** dos clientes e da empresa a fim de **garantir a continuidade** do **negócio** e **minimizar** os **riscos** de revelação ou alteração por pessoas não autorizadas. Está **relacionada** com a **proteção** existente ou necessária sobre **dados** que possuem valor para alguém ou para uma **organização**.

# FLUXO DA SEGURANÇA DA INFORMAÇÃO



# O QUE PROTEGER

- Ativos digitais
- Dados
- Conhecimento



# ATIVOS

São os elementos que sustentam a operação do negócio e podem ser classificados em:

**Tangíveis:** informações impressas, móveis, hardware (Ex.: impressoras, scanners)

**Intangíveis:** marca de um produto, nome da empresa, confiabilidade de um órgão federal

**Lógicos:** informações armazenadas em uma rede, sistema ERP (sistema de gestão integrada)

**Físicos:** galpão, sistema de eletricidade, estação de trabalho etc.

**Humanos:** funcionários.

# TIPOS DE VULNERABILIDADE

- Erros de software
- Controles ineficientes
- Processos interrompidos
- Falhas no hardware
- Mudanças nos negócios
- Erro humano.



# AMEAÇAS

**Ameaça** é algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de vulnerabilidade.

**Externas:** Tentativas de ataque e desvio de informações vindas de fora da empresa. Normalmente, essas tentativas são realizadas por pessoas com a intenção de prejudicar ou utilizar seus recursos para invadir empresas.

**Internas:** Estão presentes, independentemente das empresas estarem ou não conectadas à Internet. Podem causar desde incidentes leves até os mais graves, como a inatividade das operações da empresa.



# TIPOS DE AMEAÇAS

- **Funcionários descontentes**
- **Criminosos**
- **Terroristas**
- **Concorrentes**
- **Natureza**
- **Imprensa**
- **Hackers**




# CONTEXTO DA SEGURANÇA DE SI



# **POLÍTICA DE SEGURANÇA**

**O estabelecimento de uma Política de Segurança da Informação em sua empresa deve passar sempre por ações que norteiem esses princípios. Tal modelo deve estar amparado por um Sistema de Gestão de Segurança da Informação que precisa ser planejado, organizado, implementado, mantido e monitorado.**


**Muitas organizações não seguem esta abordagem no desenvolvimento, implementação e manutenção de seu programa. Isso é porque talvez não conheçam, ou entendam que essa abordagem é de difícil implementação ou uma perda de tempo.**



# ACORDO DE NÃO DIVULGAÇÃO

Realizado entre ao menos duas partes que destacam materiais ou conhecimentos confidenciais que desejam compartilhar para determinado propósito, mas cujo uso desejam restringir.


Um **acordo de não divulgação** cria um relacionamento confidencial entre as partes para proteger qualquer tipo de segredo comercial.

Several white lines of varying lengths and angles are drawn on the right side of the slide, extending from the middle towards the bottom right corner.


# MECANISMOS DE SEGURANÇA

**Controles físicos:** barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura que a suporta. Existem mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem guardas etc.

**Controles lógicos:** são barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado e geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Several white diagonal lines of varying lengths and thicknesses are positioned on the right side of the slide, extending from the middle towards the bottom right corner.

# APOIO DO CONTROLE LÓGICO

- **Mecanismos de criptografia:** permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
  - **Assinatura digital:** um conjunto de dados criptografados associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade
  - **Mecanismos de garantia da integridade da informação**
  - Usando funções de "**Hashing**" ou de checagem, consistindo na adição.
- 
- Several white lines of varying lengths and angles are drawn on the right side of the slide, extending from the middle towards the bottom right corner.

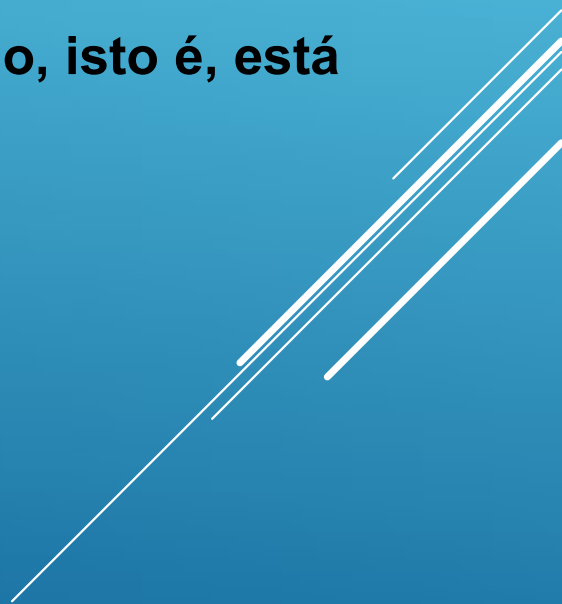
# APOIO DO CONTROLE LÓGICO

**Mecanismos de controle de acesso:** Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

**Mecanismos de certificação:** Atesta a validade de um documento

**Integridade:** Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos

**Honeypot:** É o nome dado a um software, cuja função é detectar ou de impedir a ação de um *cracker*, de um *spammer* ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Three white diagonal lines of varying lengths and thicknesses are positioned on the right side of the slide, extending from the middle towards the bottom right corner.

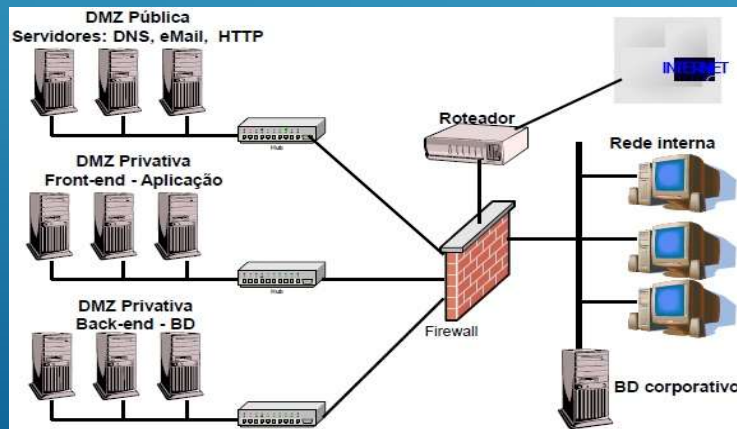
# NORMAS DE SEGURANÇA DE INFORMAÇÃO

O conceito de **Segurança da Informação** está padronizado pela norma ISO/IEC 17799:2005 (12 tópicos), influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas **ISO/IEC 27000** foram reservadas para tratar de **padrões de Segurança da Informação**, incluindo a complementação ao trabalho original do padrão inglês. A **ISO/IEC 27002:2005** continua sendo considerada formalmente como 17799:2005 para fins históricos.




# ARQUITETURA SEGURA

- **Firewalls**
- **Autenticação**
- **Criptografia**
- Sistemas de Detecção de Intrusos
- **Segurança interna dos servidores**



# QUESTÃO HUMANA

**Segurança** não é apenas uma questão técnica, mas **questão gerencial** e **humana**. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e **conscientizar** o nível gerencial da empresa e todos os seus **funcionários**.

Several white diagonal lines of varying lengths and thicknesses are positioned on the right side of the slide, extending from the middle towards the bottom right corner.

# **AULA 09**

# **SISTEMAS DE INFORMAÇÃO**

**Segurança em Sistemas  
de Informação**