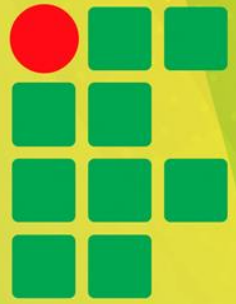
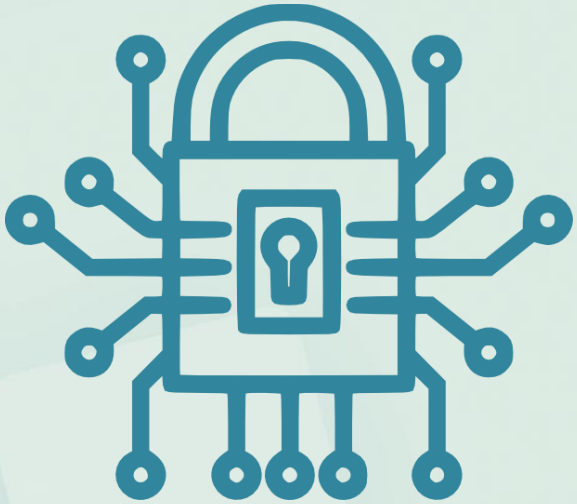


# INSTITUTO FEDERAL

Sertão Pernambucano

# Segurança da Informação



## Leis e Normas

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

# 1. Gestão de Riscos

# 1.1. Conceitos iniciais

- **Risco** de segurança é uma combinação de ameaças, vulnerabilidades e impactos. **Ameaças** são eventos que exploram **vulnerabilidades** (fragilidades) e podem causar **danos**. O **impacto** é a consequência de uma vulnerabilidade ter sido explorada por uma ameaça.

# 1.1. Conceitos iniciais

- A **gestão** de riscos compreende todas as ações tomadas para controlar os riscos em uma organização, incluindo análise/avaliação, tratamento, aceitação e comunicação dos riscos;

# 1.1. Conceitos iniciais

- A **análise de riscos** identifica e estima riscos, considerando o uso sistemático de informações. Engloba a análise de ameaças, vulnerabilidades e impactos, e é considerada o ponto-chave da política de segurança da informação de uma organização;

# 1.1. Conceitos iniciais

- A **avaliação de riscos** compara o risco estimado na análise com critérios predefinidos, objetivando identificar a importância do risco para a organização;
- A **aceitação de riscos** engloba o levantamento do nível aceitável de riscos para uma organização de acordo com seus requisitos específicos de negócio e segurança;

# 1.1. Conceitos iniciais

- O **tratamento de riscos** corresponde à seleção e implementação de medidas para modificar um dado risco.
- A **comunicação de riscos** envolve as iniciativas de divulgação dos riscos aos funcionários, dirigentes e terceiros (estes últimos, quando cabível e necessário).

# 1.2. Questões determinantes

- Para realizar uma efetiva gestão de riscos, é preciso levantar, inicialmente, as ameaças e impactos, a probabilidade de concretização de ameaças e os riscos potenciais.

# 1.2. Questões determinantes

- É recomendável classificar os riscos segundo os critérios:
  - **nível de importância**;
  - **grau de severidade de perdas;**
  - **custos envolvidos com a prevenção ou recuperação após desastres.**

# 1.3. Implementação

- Implementar em três níveis:

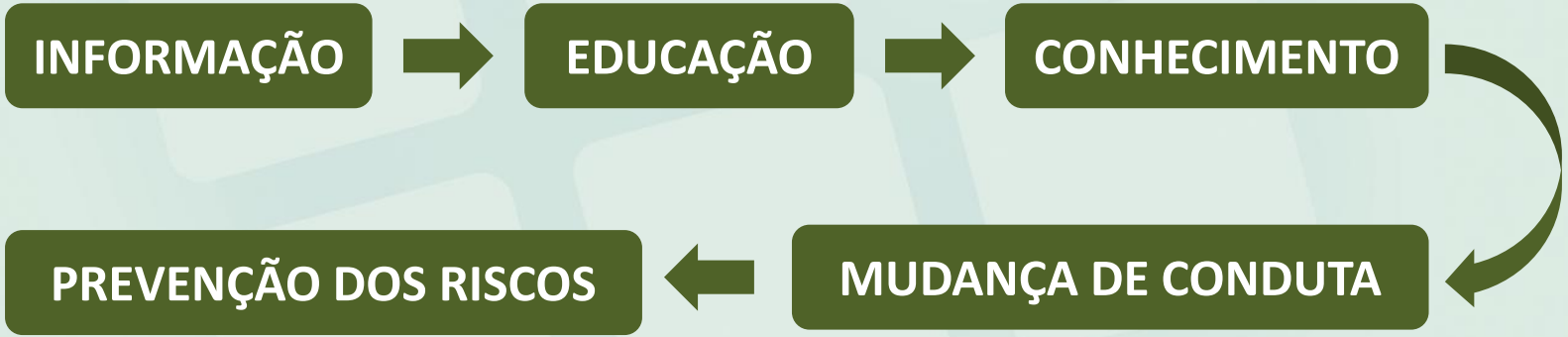
**1º - TECNOLOGIA**

**2º - PROCESSO**

**3º - PESSOAS**

# 1.3. Implementação

- Sequência para a mudança de conduta e prevenção dos riscos:



# 1.4. Análise e avaliação de riscos

- A análise/avaliação de riscos envolve a **identificação, quantificação e qualificação dos riscos de segurança da informação**, tendo como base os objetivos da organização. Envolve ainda a priorização de riscos, considerando os critérios de riscos aceitáveis.

# 1.4. Análise e avaliação de riscos

- A análise/avaliação de riscos envolve a **identificação, quantificação e qualificação dos riscos de segurança da informação**, tendo como base os objetivos da organização. Envolve ainda a priorização de riscos, considerando os critérios de riscos aceitáveis.

# 1.5. Analisando os riscos

- **Considerar:**
  - Danos causados por falhas de segurança.
  - Probabilidade de falhas ocorrerem.
- **Questões relevantes:**
  - O que proteger?
  - Quais as vulnerabilidades e ameaças?
  - Como analisar?

# 1.5. Analisando os riscos

- **Resultado:**
  - Dados que guiam a gestão de riscos.

- **O que proteger?**
- **Quais as vulnerabilidades e ameaças?**
- **Como analisar?**

# 1.6. O que proteger?

- **Deve-se analisar as ameaças e vulnerabilidades antes.**

**Ativos típicos:**

- **Hardware.**
- **Software.**
- **Dados.**
- **Pessoas.**

- **Documento.**
- **Sistemas de informação.**
- **Valores intangíveis.**
- **Contratos etc..**

# 1.7. Vulnerabilidades e ameaças

- Determinar as vulnerabilidades e ameaças aos ativos a proteger.
- Determinar o impacto.

- Considerar:
  - Compromisso com a informação.
  - Confidencialidade.
  - Integridade.
  - Disponibilidade.

# 1.7. Vulnerabilidades e ameaças

- **Exemplos de ameaças típicas:**
  - Desastres naturais.
  - Falhas no fornecimento de energia elétrica.
  - Roubo.
  - Ameaças programadas.
  - Falhas de hardware.
  - Falhas de software.
  - Erros humanos.

# 1.7. Vulnerabilidades e ameaças

- **Analisar considerando:**
  - Custos.
  - Nível de proteção requerido.
  - Facilidades de uso.
- **A análise de risco pode ser:**
  - Qualitativa.
  - Quantitativa.

# 1.8. Análise de impactos

- Exemplo de classificação:
  - 0 - irrelevante.
  - 1 - efeito pouco significativo.
  - 2 - sistemas não disponíveis por determinado período.
  - 3 - perdas financeiras.
  - 4 - efeitos desastrosos, sem comprometimento dos negócios.
  - 5 - efeitos desastrosos, comprometendo os negócios.

# 1.9. Avaliação de riscos

- Modos:
  - Qualitativo.
  - Quantitativo.

- Conhecer os impactos é relevante.

# 1.10. Tratamento de riscos de segurança

- Compreende a colaboração entre partes:
  - Dirigentes, funcionários, auditores, consultores etc.

# 1.10. Tratamento de riscos de segurança

- Objetivos:
  - Aprovar metodologias e procedimentos de segurança da informação.
  - Assegurar a conformidade com a política de segurança.
  - Coordenar a implantação de controles.
  - Educar para a segurança da informação.

# 1.10. Tratamento de riscos de segurança

- Aspectos importantes no tratamento de riscos:
  - Metodologias e procedimentos de segurança da informação.
  - Conformidade com a política de segurança.
  - Medidas de segurança (Corretivas, Preventivas e Orientativas)

# 1.10. Tratamento de riscos de segurança

- Deve-se ainda atentar durante a fase do tratamento do risco para segmentos importantes para que sejam implementados controles e que devem constar do escopo do tratamento:
  - Recursos humanos.

# 1.10. Tratamento de riscos de segurança

- Controles de acesso lógico.
- Controles de acesso físico.
- Controles ambientais.
- Comunicações.
- Continuidade de serviços.
- Contratação de serviços de terceiros.
- Controle organizacional.
- Controle de mudanças.

# 1.10. Tratamento de riscos de segurança

- áreas são consideradas essenciais à organização na garantia de seus objetivos de negócio:
  - Segurança de Recursos Humanos.
  - Segurança de acesso.
  - Segurança nas comunicações.
  - Segurança e negócios.

# 1.11. Tratamento de riscos na segurança de Recursos Humanos

- As pessoas devem ter consciência de suas responsabilidades e dos riscos e ameaças de segurança. Deve-se ainda atentar para eventos adversos que representem riscos.

# 1.12. Tratamento de riscos na segurança de acesso

- Atentar para os fatores de risco.
- Considerar a análise/avaliação de riscos:
  - Definir perímetros de segurança.
  - Proteger equipamentos e dispositivos de armazenamento.
  - Minimizar riscos de corrupção de sistemas operacionais.
  - Reduzir riscos de ameaças físicas.

# 1.12. Tratamento de riscos na segurança de acesso

- Educação e conscientização são cruciais.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de riscos relacionados ao controle de acesso lógico inadequado:
- Alteração não autorizada de dados e aplicativos.
- Divulgação não autorizada de informações.
- Introdução de códigos maliciosos.

# 1.12. Tratamento de riscos na segurança de acesso

- Impactos:
  - Perdas financeiras decorrentes de fraudes, restaurações etc.
  - Inviabilidade de continuidade dos negócios.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de tratamentos para um adequado controle de acesso lógico:
  - Restringir e monitorar o acesso a recursos críticos.
  - Utilizar criptografia.
  - Não armazenar senhas em logs.

# 1.12. Tratamento de riscos na segurança de acesso

- Conscientizar os usuários para que não divulguem suas senhas.
- Conceder acesso apenas aos recursos necessários às atividades dos funcionários.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de riscos relacionados ao controle de acesso físico inadequado:
  - Roubo de equipamentos.
  - Atos de vandalismo.

# 1.12. Tratamento de riscos na segurança de acesso

- Impactos:
  - Perdas financeiras.
  - Facilidades para ataques contra controles de acesso lógico.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de tratamentos para um adequado controle de acesso físico:
  - Identificar funcionários e visitantes.
  - Controlar a entrada/saída de equipamentos.
  - Supervisionar a atuação da equipe de limpeza, manutenção e vigilância.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de riscos relacionados ao controle ambiental inadequado:
  - Desastres naturais.
  - Falhas no fornecimento de energia elétrica.

# 1.12. Tratamento de riscos na segurança de acesso

- Impactos:
  - Danos em equipamentos.
  - Indisponibilidade de serviços.
  - Perdas financeiras.

# 1.12. Tratamento de riscos na segurança de acesso

- Exemplos de tratamentos para um adequado controle ambiental:
  - Uso de material resistente a fogo.
  - Manutenção de número suficiente de extintores de incêndio.
  - Controle de focos de problemas com água.
  - Controle de temperatura, umidade e ventilação.
  - Manutenção da limpeza e conservação do ambiente.

# 1.13. Tratamento de riscos na segurança das comunicações

- Disponibilizar medidas de segurança adequadas às comunicações.
  - Considerações:
  - Proteção de conexões a serviços de rede.
  - Garantir a segurança para a comunicação wireless.

# 1.14. Tratamento de riscos e negócios

- Proteger recursos e informações para atingir objetivos de negócio. Atentar para:
  - Aplicações críticas aos negócios.
  - Controlar novos contratos e parcerias.
  - Identificar necessidades de integridade das mensagens.
  - Estabelecer uma política para uso adequado de criptografia.
  - Identificar e reduzir riscos à continuidade de negócios.

# 1.15. Comunicação de riscos

- Ativos são elementos essenciais ao negócio da organização. q
- Ativos devem ser inventariados.
- Todo ativo deve ter um responsável por manter sua segurança.

# Obrigado!
# Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano