UNINOVE
Universidade Nove de Julho

PPGI

# Disciplina
# Segurança da Informação

Aula 04 – Análise de Riscos

Professor: João Rafael
Email: joao.rafael@uni9.pro.br

São Paulo
2025

# Análise de Riscos

UNINOVE
Universidade Nove de Julho

# Introdução - Análise de Risco

- Devido a necessidade de proteger seus ativos de informação, as organizações passaram a implementar uma série de **medidas** e **controles internos** que as ajudassem a **identificar quais os possíveis riscos que um ativo de informação está sujeito**. Pode-se citar como exemplos de ativo de informação:

  - **Dispositivos Eletrônicos:** Computadores, Notebooks e Servidores;
  - **Dispositivos de Rede:** Roteadores, PABX, Access Point, Switches, Modems;
  - **Dispositivos de Armazenamento:** Mídias Magnéticas, PenDrives, DVDs, HD's Externos;
  - **Documentações:** Relatórios, Registros, Dados de contatos.

UNINOVE
Universidade Nove de Julho

# Como Realizar uma Análise de Risco

- Após compreender a **importância de proteger os ativos de informação**, é necessário descobrir quais são seus **pontos fracos** e então, definir quais controles de segurança devem ser implantados. Esta atividade **é chamada Análise de Risco**.

- Quando não se sabe o que deve ser protegido e contra o que deve-se proteger, é mais difícil **implantar medidas de segurança eficazes.** A partir do momento que as organizações identificam os seus riscos e ameaças, torna-se possível **planejar as ações**.

# Como Realizar uma Análise de Risco

- Analisar riscos é uma tarefa que **difere** de **profissional** para **profissional**, assim como de organização para organização. Cada um enxerga o risco sob um determinado **ponto de vista**.

# Principais Componentes Relacionados na Análise de Riscos

UNINOVE
Universidade Nove de Julho

# Principais Componentes - Análise de Risco

- Os principais componentes relacionados com a tarefa de Análise de Riscos são:
  - Riscos
  - Ameaças
  - Vulnerabilidades
  - Impactos
  - Ativos de Informação
  - Controles de Segurança da Informação

UNINOVE
Universidade Nove de Julho

# Principais Componentes - Análise de Risco

- **Riscos:** Trata-se de um **perigo** ou **possibilidade de perigo**. É a probabilidade de acontecer algo, pela exploração dos pontos fracos de um determinado ativo de informação ou ambiente, ocasionando perda de confidencialidade, integridade e disponibilidade.

- **Ameaças:** São intenções de causar **mal**, **danos** e **prejuízos** capazes de gerar incidentes inesperados. Uma ameaça costuma ser **facilmente detectada**, mas sua ocorrência é **dificilmente evitada**. As ameaças podem ser classificadas em três tipos: ***Naturais***, ***Intencionais*** e ***Não-Intencionais***.

UNINOVE
Universidade Nove de Julho

# Análise de Risco – Tipos de Ameaças

- **Ameaças Naturais**: Representadas por fenômenos da natureza, como Enchentes, incêndios naturais, aquecimento, poluição, vendavais, terremotos, etc.

- **Ameaças Intencionais:** Representadas por ações propositais causadas por agentes humanos internos ou externos à organização, como: invasões, espionagem, furto, disseminação de malwares, etc.

- **Ameaças Não-intencionais:** Representadas por ações que ocorrem por falta de conhecimento técnico dos envolvidos, como: Alterações incorretas em recursos produtivos, envio de informações sensíveis por engano para pessoas não-autorizadas, descarte incorreto de informações, etc.

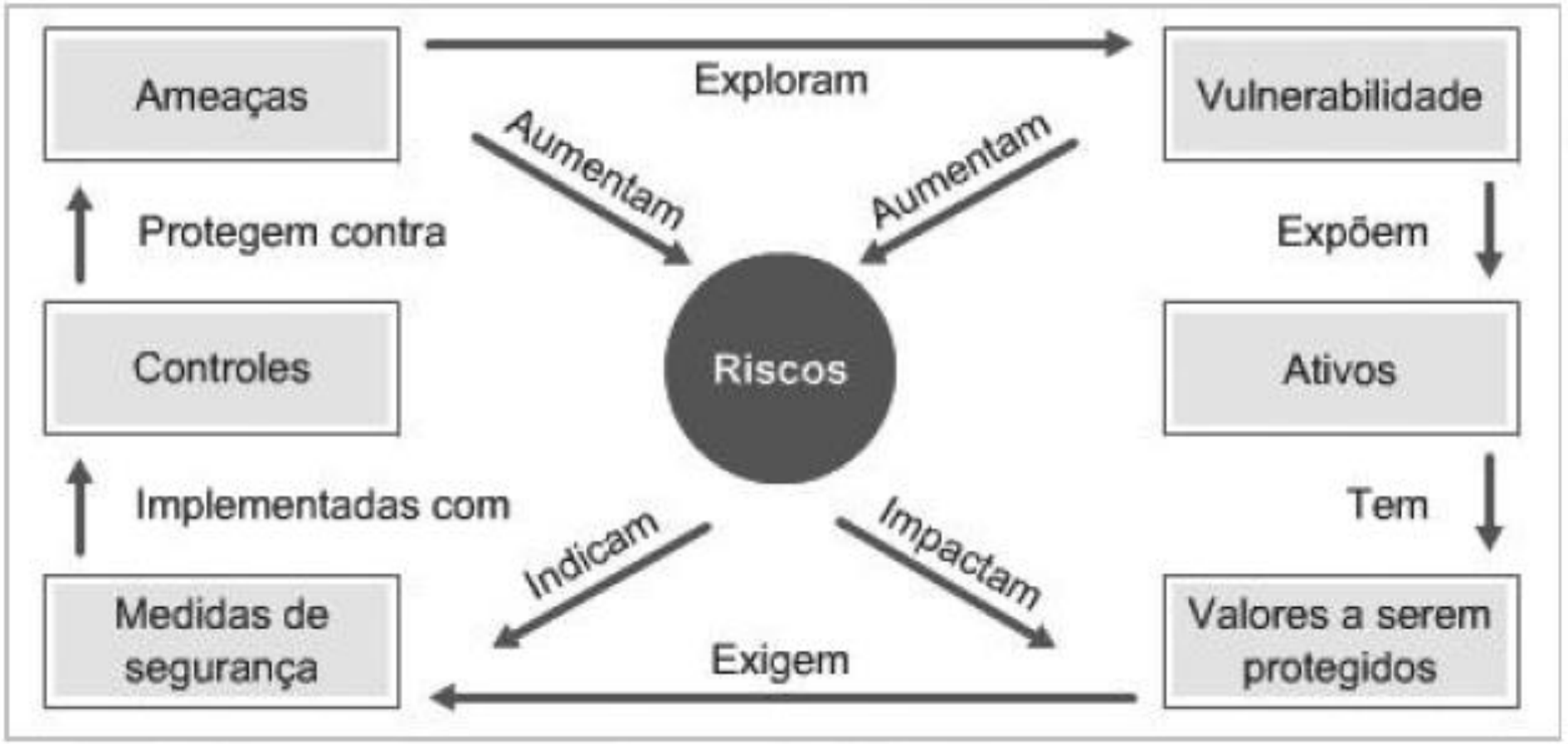
UNINOVE
Universidade Nove de Julho

# Principais Componentes - Análise de Risco

- **Vulnerabilidades:** Trata-se dos **pontos fracos** ou **falhas** presentes em um ativo de informação. A exploração de vulnerabilidades por uma determinada ameaça, representa um **risco** para a organização. São exemplos de vulnerabilidade: softwares desatualizados, informações confidenciais disponíveis publicamente, dispositivos online com páginas de setup públicas, etc.

- **Impactos:** É o conceito utilizado para medir os efeitos positivos ou negativos, que uma determinada ação pode causar. São exemplos de impactos: Perdas financeiras, multas, sanções, danos a imagem da organização, etc.

# Principais Componentes - Análise de Risco



# Como é realizada uma Análise de Riscos?

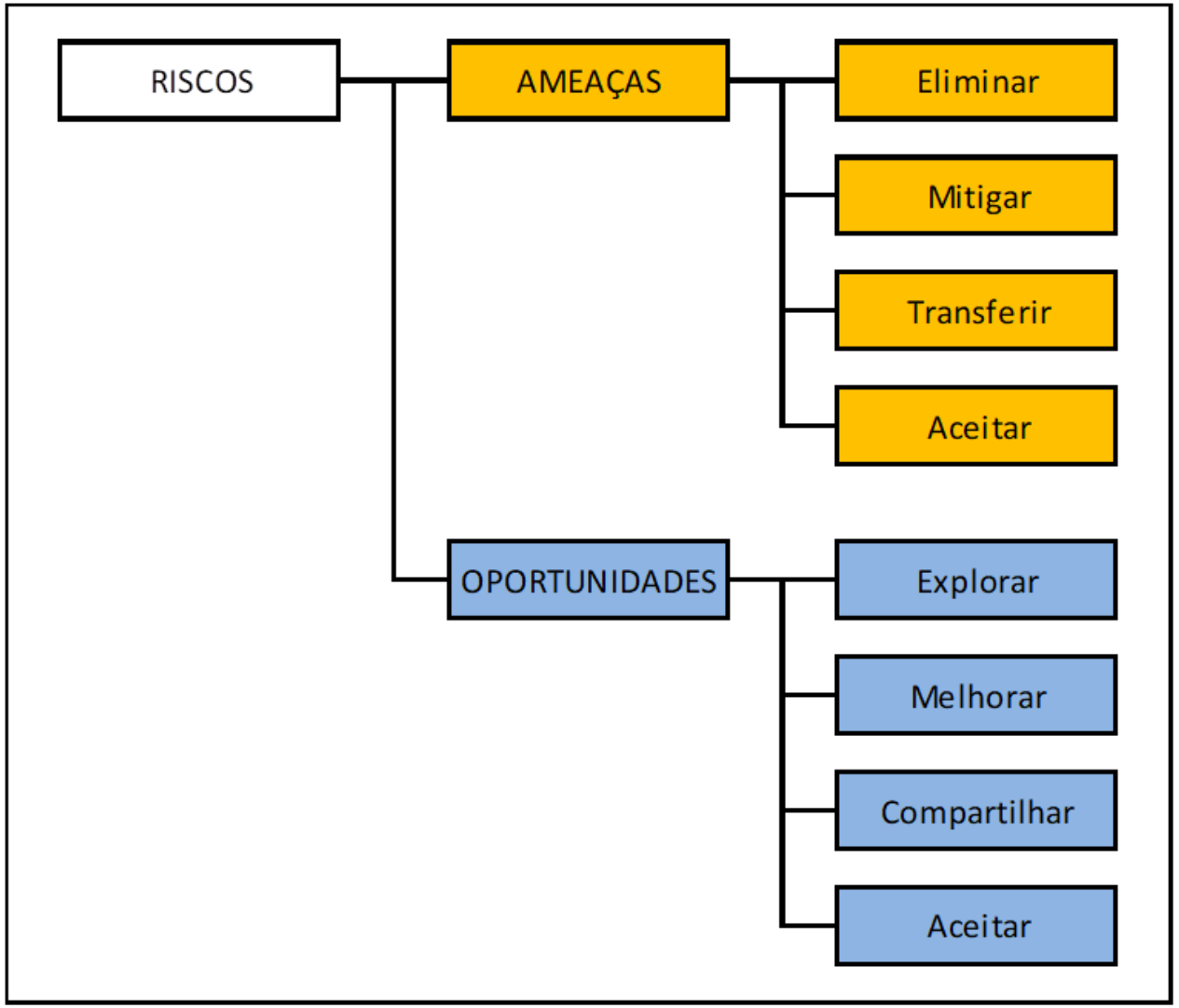
UNINOVE
Universidade Nove de Julho

# Como é Realizada a Análise de Risco

- A **Análise de Riscos** tem por objetivo responder a uma série de perguntas necessárias para a identificação de possíveis riscos para ativos de informação, ambientes e/ou organizações. São exemplos de perguntas:

  - O que pode acontecer de errado?
  - Com que frequência isso pode acontecer?
  - Quais as suas possíveis consequências?
  - O que precisa ser feito para que se possa reduzir os riscos?
  - Devo ou não aceitar esse risco?
  - O que, como e onde devo priorizar as ações de segurança?
  - O que, quando e como devo ignorar um incidente de segurança?

# Como é Realizada a Análise de Risco?



# Técnicas e Práticas para Análise de Riscos

# Técnicas e Práticas - Análise de Risco

- Remoção de Subjetividade
- Análise Quantitativa e Análise Qualitativa
- Estudo de Operabilidade de Riscos (HAZOP)
- Análise Preliminar de Perigos (APP)
- Análise Preliminar de Riscos (ARP)
- **Diagrama de Causa e Efeito de Ishikawa (Espinha de Peixe)**
- **Matriz GUT**
- **Matriz de Probabilidade e Impacto**

UNINOVE
Universidade Nove de Julho

# Técnicas e Práticas - Análise de Risco

- **Remoção de Subjetividade:** Esta análise não é precisa, pois é feita através de suposições. Sem ter os meios adequados para provar os riscos, esta análise busca atingir resultados aproximados do real.

- **Análise Quantitativa:** Esta análise busca quantificar valores para cada um dos riscos identificados. Para isso, busca-se entender qual o valor de cada ativo de informação existente na organização.

- **Análise Qualitativa:** Esta análise busca utilizar critérios de estimação de impactos para cada risco que venha acontecer. Esta estimação abrange impactos tangíveis e intangíveis.

# Técnicas e Práticas - Análise de Risco

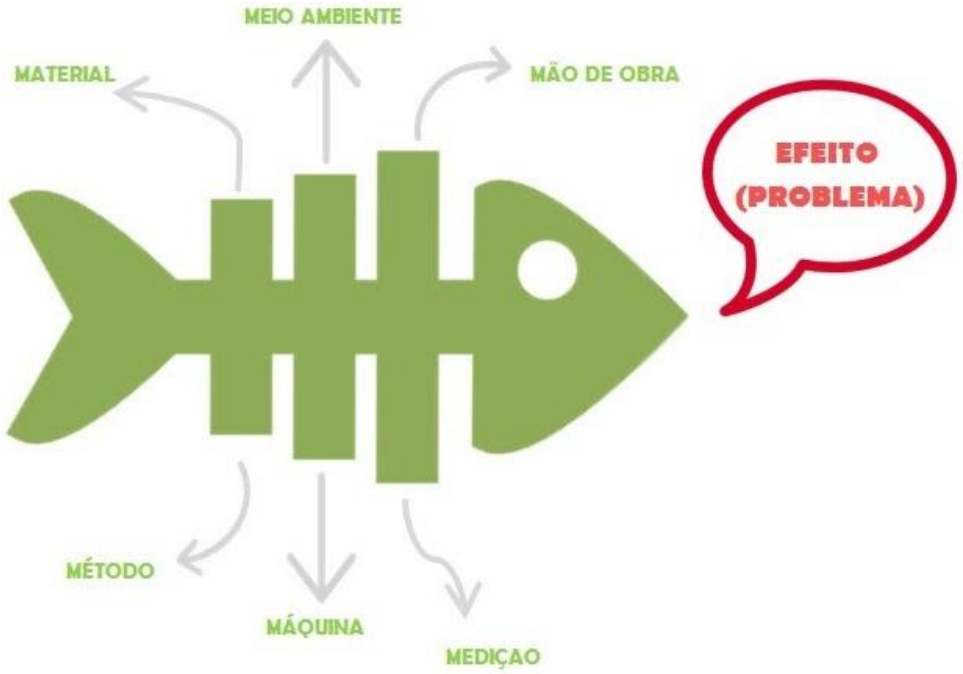
- **Estudo de Operabilidade de Riscos (HAZOP):** Esta análise cria um conjunto de medidas para reduzir / eliminar riscos em processos, abrangendo também os erros operacionais.

- **Análise Preliminar de Perigos (APP):** Esta análise busca identificar os possíveis acidentes que podem ocorrer em uma determinada instalação de equipamentos ou configuração de ambientes.

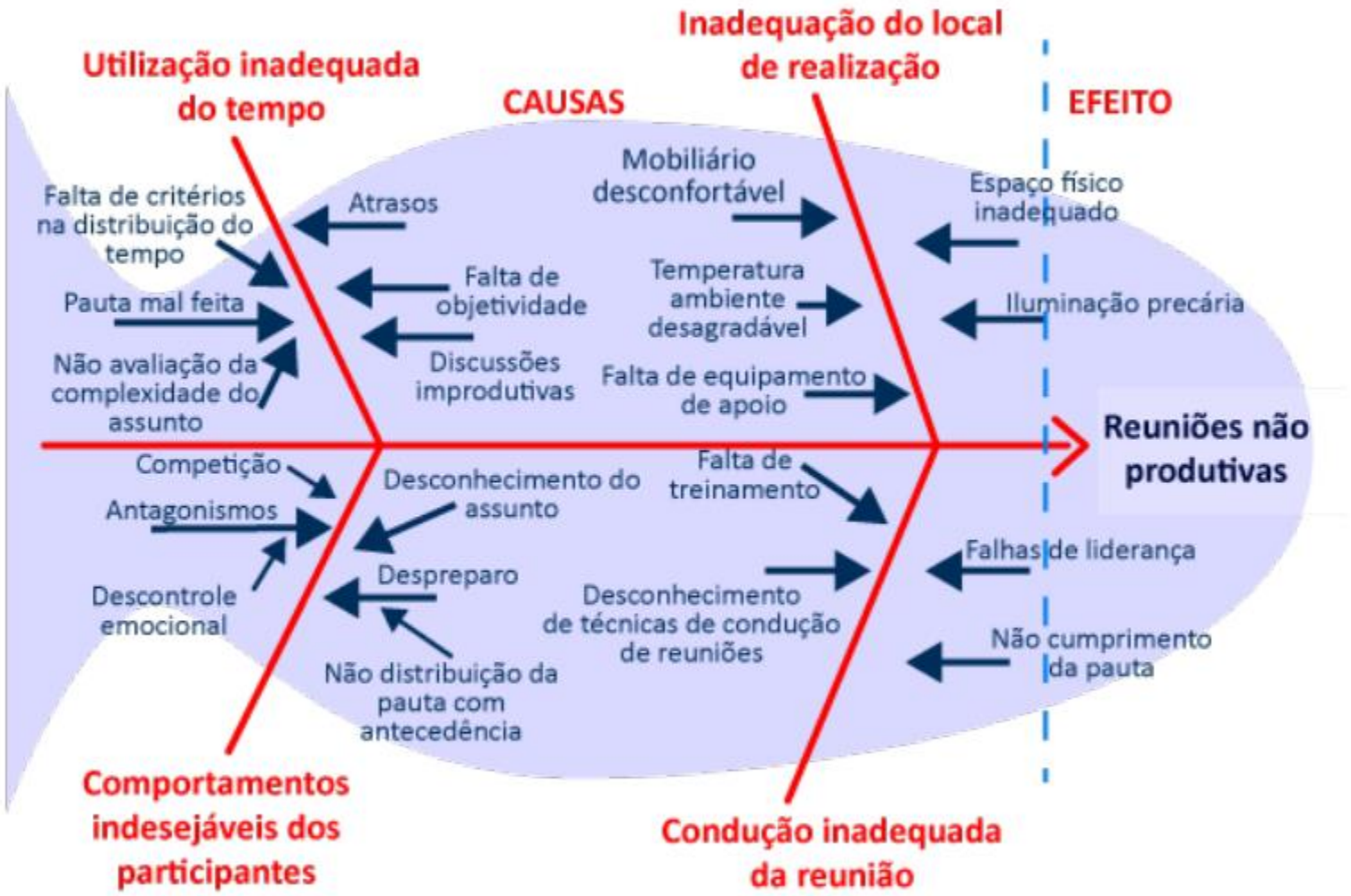
- **Análise Preliminar de Riscos (APR):** Esta análise busca executar uma revisão geral de riscos já mapeados que fazem parte da execução de um determinado projeto.

# Técnicas e Práticas - Análise de Risco

- **Diagrama de Causa e Efeito de Ishikawa (Espinha de Peixe):** Esta análise gráfica é comumente usada para encontrar a origem de um problema e seus possíveis riscos. Neste diagrama, o ***"problema"*** é tratado como ***"efeito"*** e suas influências, a ***"causa"***.



# Diagrama de causa e efeito de Ishikawa (Espinha de Peixe)



UNINOVE
Universidade Nove de Julho

# Técnicas e Práticas - Análise de Risco

- **Matriz GUT:** Trata-se de uma ferramenta de "**Priorização**" para resolução de problemas. Para cada problema (*Risco*), atribui-se um valor (de 1 a 5) para cada uma das três dimensões da Matriz GUT: **Gravidade**, **Urgência** e **Tendência**. Por fim, todos os três valores são Multiplicados, para assim, gerar uma classificação em **ordem crescente**, a fim de criar uma lista de prioridades.

  - **Gravidade:** Impacto do problema sobre coisas, pessoas, resultados, processos ou organização.
  - **Urgência:** É a relação com o tempo disponível para resolver o problema.
  - **Tendência:** É o potencial de crescimento / ocorrência do problema.

UNINOVE
Universidade Nove de Julho

# Análise de Risco – Matriz GUT

| Gravidade | Urgência | Tendência |
|---|---|---|
| 5 Extremamente grave. | 5 Precisa de ação imediata. | 5 Irá piorar rapidamente se nada for feito. |
| 4 Muito grave. | 4 É urgente. | 4 Irá piorar em pouco tempo se nada for feito. |
| 3 Grave. | 3 O mais rápido possível. | 3 Irá piorar. |
| 2 Pouco grave. | 2 Pouco urgente, o prazo ainda é longo. | 2 Irá piorar a longo prazo. |
| 1 Sem gravidade. | 1 Fica tranquilo, pode esperar! | 1 A situação não tem tendência de piorar. |

UNINOVE
Universidade Nove de Julho

# Análise de Risco – Exemplo de Matriz GUT

| Exemplo de uma Matriz de Priorização G.U.T. | | | | | |
|---|---|---|---|---|---|
| Problemas | Gravidade | Urgência | Tendência | Total | Priorização |
| Atraso na entrega dos Servidores | 4 | 4 | 3 | 48 | 2º |
| Parada do fornecimento do link de internet | 3 | 2 | 1 | 6 | 4º |
| Ataque de vírus na rede de computadores | 4 | 4 | 4 | 64 | 1º |
| Falta de equipamento de Nobreak para proteção dos Servidores | 5 | 2 | 3 | 30 | 3º |

UNINOVE
Universidade Nove de Julho

# Técnicas e Práticas - Análise de Risco

- **Matriz de Probabilidade e Impacto:** Semelhante a Matriz GUT, trata-se de uma ferramenta que apoia a tarefa de priorização e classificação de riscos. Para isso, em cada risco, calcula-se os valores de **Probabilidade** e **Impacto**.

  - **Impacto:** Impacto do problema sobre coisas, pessoas, resultados, processos ou organização.
  - **Probabilidade:** É o potencial de crescimento / ocorrência do problema.

# Análise de Risco – Matriz de Probabilidade e Impacto

| Probabilidade / Impacto | Sem Impacto | Leve | Médio | Grave | Gravíssimo |
|---|---|---|---|---|---|
| Quase certo | Risco Elevado | Risco Elevado | Risco Extremo | Risco Extremo | Risco Extremo |
| Alta | Risco Moderado | Risco Elevado | Risco Elevado | Risco Extremo | Risco Extremo |
| Média | Risco Baixo | Risco Moderado | Risco Elevado | Risco Extremo | Risco Extremo |
| Baixa | Risco Baixo | Risco Baixo | Risco Moderado | Risco Elevado | Risco Extremo |
| Raro | Risco Baixo | Risco Baixo | Risco Moderado | Risco Elevado | Risco Elevado |

# Referências

# Referências e Links Úteis


- COELHO, Flávia Estélia Silva, BEZERRA, Edson Kowask, ARAÚJO, Luiz Geraldo Segadas. Gestão da Segurança e da Informação: NBR 27001 e NBR 27002. Escola Superior de Redes, 2013, 212p.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação . Rio de Janeiro: Axcel Books, 2000.
- FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.
- NAKAMURA, Emílio Tissato; GEUS, Paulo. Lício de. Segurança de redes em ambientes cooperativos. São Paulo: Berkeley, 2002.
- SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003.
- VINTEN, Gerald. Auditing and Security. AS/400, NT, Unix, Networks, and Disaster Recovery Plans. Managerial Auditing Journal, v. 17, n. 5, p. 289-290, 2002.