SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE III – GESTÃO DE RISCOS EM AMBIENTES DA INFORMAÇÃO

PUC Minas
Virtual

3.2 – MODELOS DE GESTÃO DE RISCO

PUC Minas
Virtual

3.2.2 – FAMÍLIA ISO 27000

FAMÍLIA ISO 27000

- Os padrões **ISO/IEC 27001:2017** que apresentam diretrizes para a implantação de Sistemas de gerenciamento de segurança da informação – Requisitos e;
- **ISO/IEC 27002:2017**, que trata das Técnicas de segurança – Código de prática para controles de segurança da informação.
- Juntos fornecem uma base para as organizações desenvolverem sua estrutura de gerenciamento de segurança da informação com foco no gerenciamento e proteção de seus importantes ativos de negócios.

ISO 27001

- É um **padrão de requisitos** utilizado para **certificações** de Sistemas de Gerenciamento de Segurança da Informação **(SGSI)** de terceiros credenciados.
- A rota desta certificação envolve auditoria do **SGSI** por um organismo de certificação credenciado.
- Desta forma há a garantia de que eles tenham processos e sistemas de gerenciamento aderentes ao modelo e que os mecanismos implantados estejam em conformidade com os requisitos especificados na **ISO/IEC 27001**.

ISO 27002

- É um documento de **orientação** onde se **fornece** um conjunto abrangente de **controles de melhores práticas** para segurança da informação e orientação sobre como implantar.
- Adotam-se esses controles como parte do **processo de tratamento de riscos** especificado na norma **ISO/IEC 27001**, para gerenciar os riscos que enfrentam em seus ativos de informação.

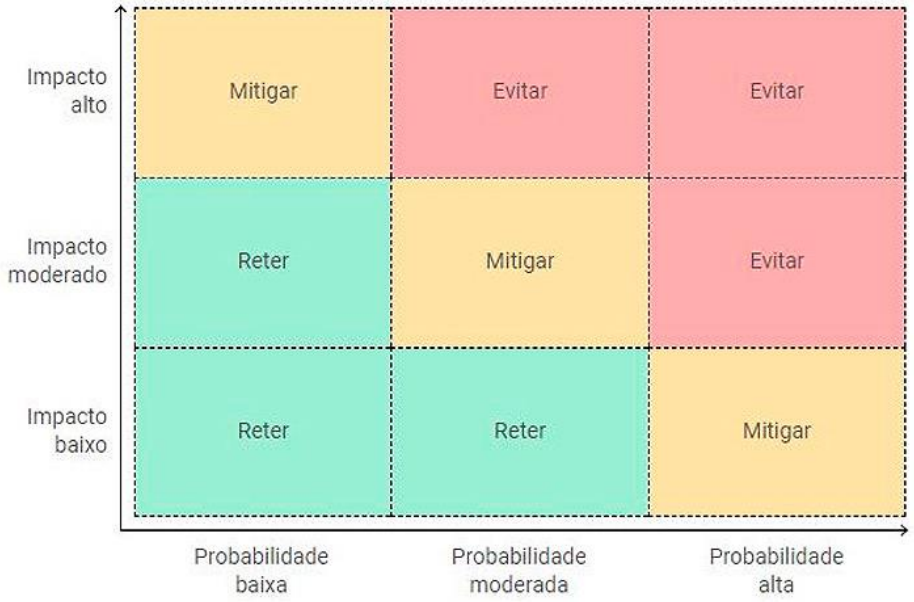
COMO FUNCIONA A IMPLANTAÇÃO

- A ISO/IEC 27001 é dividida em duas partes principais
- **Requisitos para processos em um SGSI:** que são descritos nas Cláusulas 4–10 (o corpo principal do texto); e
- **A lista de controles SGSI**, que é fornecida no **Anexo A**.
- Esses controles são descritos com mais detalhes na **ISO/IEC 27002**.

CONTROLES INTERNOS

- Quando uma empresa passa por este tipo de certificação é importante garantir que haja a conformidade constante destes requisitos.
- A forma de alcançarmos sucesso neste objetivo é a implantação de controles internos baseados nos requisitos da certificação.
- É uma conversa que envolve, CEO, Conselho de administração, Acionistas e empresas Auditoria independentes que são contratadas para avaliar o cumprimento destes requisitos.

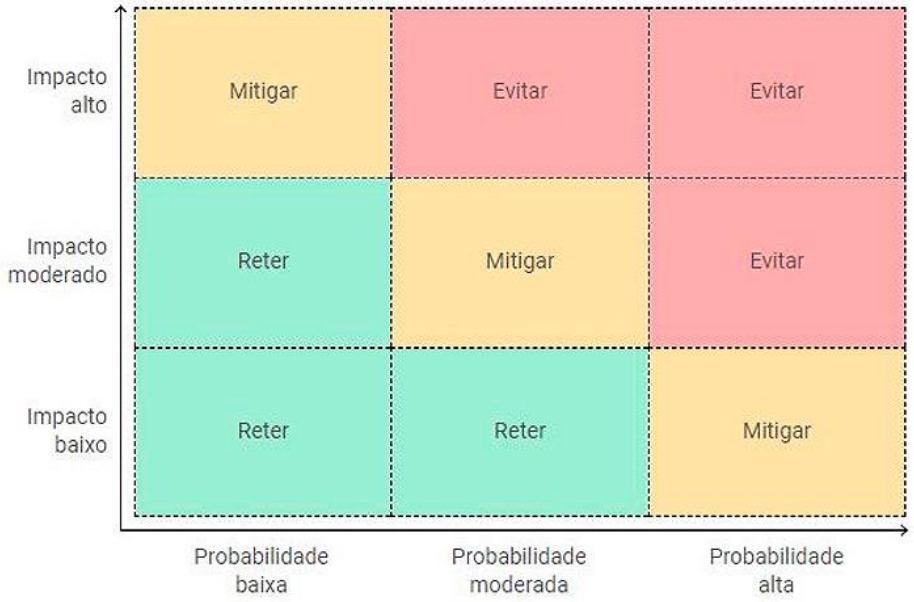
MATRIZ DE RISCO



Fonte: SESTREM,2022

- A partir da lista de riscos que for elencada no processo de construção do **SGSI, identificamos os diferentes níveis e pesos de cada risco.**
- A partir desta classificação construímos uma **Matriz de Risco** que é uma representação gráfica de fácil entendimento que exibe a criticidade dos riscos que são tratados pela organização.

MATRIZ DE RISCO



Fonte: SESTREM,2022

- Os riscos são a combinação de dois elementos: **probabilidade:** mede o quão fácil ou difícil é que um determinado risco ocorra dentro da empresa e **impacto:** consequências que determinado risco pode trazer para o negócio.
- A matriz de riscos permite que a equipe **concentre sua atenção** e recursos **nos riscos que mais impactam o negócio**, a partir da priorização das ameaças.

REFERENCIAS BIBLIOGRÁFICAS

BRASILIANO, Antonio Celso Ribeiro**.** Risk Assessment em Cybersecurity Risks: Qual o produto?. Disponível em: <https://www.brasiliano.com.br/40-risk-assessment>. Acesso em: 21 Out. 2022.

BRUMFIELD Cynthia, HAUGLI Brian. Cybersecurity Risk Management. O'REILLY, 2021.

LEBLANC Jonathan, MESSERSCHMIDT Tim. Identity and Data Security for Web Development. . O'REILLY, 2016.

SESTREM, Thatiana**.** Matriz de risco: o que é e como implementar na sua empresa. Disponível em: <https://qualyteam.com/pb/blog/matriz-de-risco/>. Acesso em: 25 Out. 2022.


PUC Minas
Virtual