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

3.2.1 – NIST FRAMEWORK

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

O NIST

- *National Institute of Standards and Technology* **(NIST):** é uma organização de pesquisa que produz **patentes**, **avanços técnicos**, **documentação** e recomendações por meio de ampla consulta a especialistas em várias áreas, repleta de alguns dos principais cientistas do mundo e que produziu muitos vencedores do Prêmio Nobel.

O FRAMEWORK DO NIST

- **NIST** *Cybersecurity Framework* **(NCF)** é resultado de um esforço que sintetizou o melhor pensamento dos especialistas em segurança cibernética.
- A ideia é tentar incorporar todas as **melhores práticas** de **gerenciamento** e **mitigação** de riscos com uma meta ambiciosa no complexo campo de segurança cibernética.
- Neste documento há uma preocupação extrema em **colaboração** para definir estas melhores práticas com um **conjunto de padrões** para gerenciamento dos riscos.

O FRAMEWORK DO NIST

- Suponha que uma organização não tenha uma iniciativa de gerenciamento de riscos de segurança cibernética ou um conjunto de práticas de segurança cibernética em vigor, a estrutura apresentada pelo **NIST** deve servir como um bom ponto de partida para o desenvolvimento desse programa ou dessas práticas.
- O *roadmap* base para que consigamos atingir os objetivos no processo de gerenciamento de riscos em segurança cibernética passam por algumas atividades:

O FRAMEWORK DO NIST

- **Determinar o risco de estrutura:** estudar e formalizar quanto risco sua organização está disposta a assumir em relação a determinadas **restrições e objetivos** da alta administração.
- **Avalie o risco:** determinar a importância de vários ativos, saber quais são protegidos e o grau de vulnerabilidade de cada um dos ativos, no nosso caso os dados.

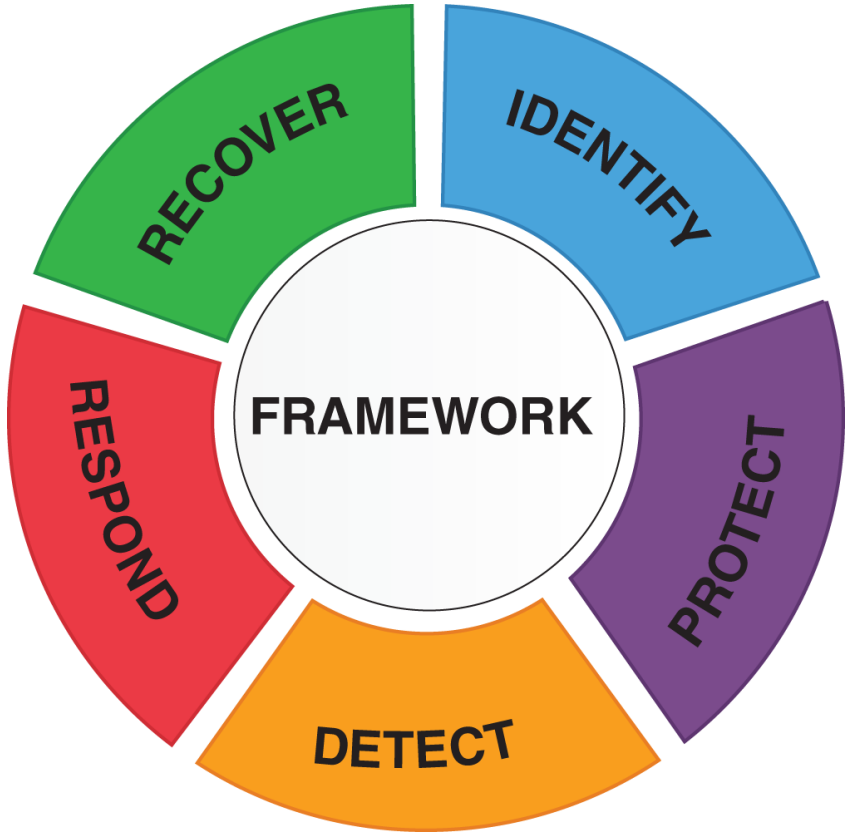
O FRAMEWORK DO NIST

- **Responder ao risco uma vez determinado:** elaborar e definir os planos de ação se os riscos se transformarem em realidades adversas.
- **Monitore os riscos continuamente:** verificar os planos de risco de forma a garantir que a implementação e/ou a atualização aconteça à medida que as situações mudem com base no **monitoramento contínuo** ou periódico desses planos.

O FRAMEWORK DO NIST

- Com estes passos inicia-se o processo de atribuição de responsabilidades baseando-se perdas dos riscos que foram mapeados.
- A recomendação dos especialistas é que a **propriedade do risco** recaia sobre os **executivos** responsáveis pelas devidas disciplinas ou segmentos de negócio cobrindo os custos de a ameaça se materializar.

O FRAMEWORK DO NIST



Fonte: BRUMFIELD, HAUGLI, 2021

- *Framework Core* é um conjunto de atividades destinadas a organizar iniciativas de segurança cibernética para alcançar resultados específicos.
- Tem cinco funções: Identificar, Proteger, Detectar, Responder e Recuperar.

O FRAMEWORK DO NIST

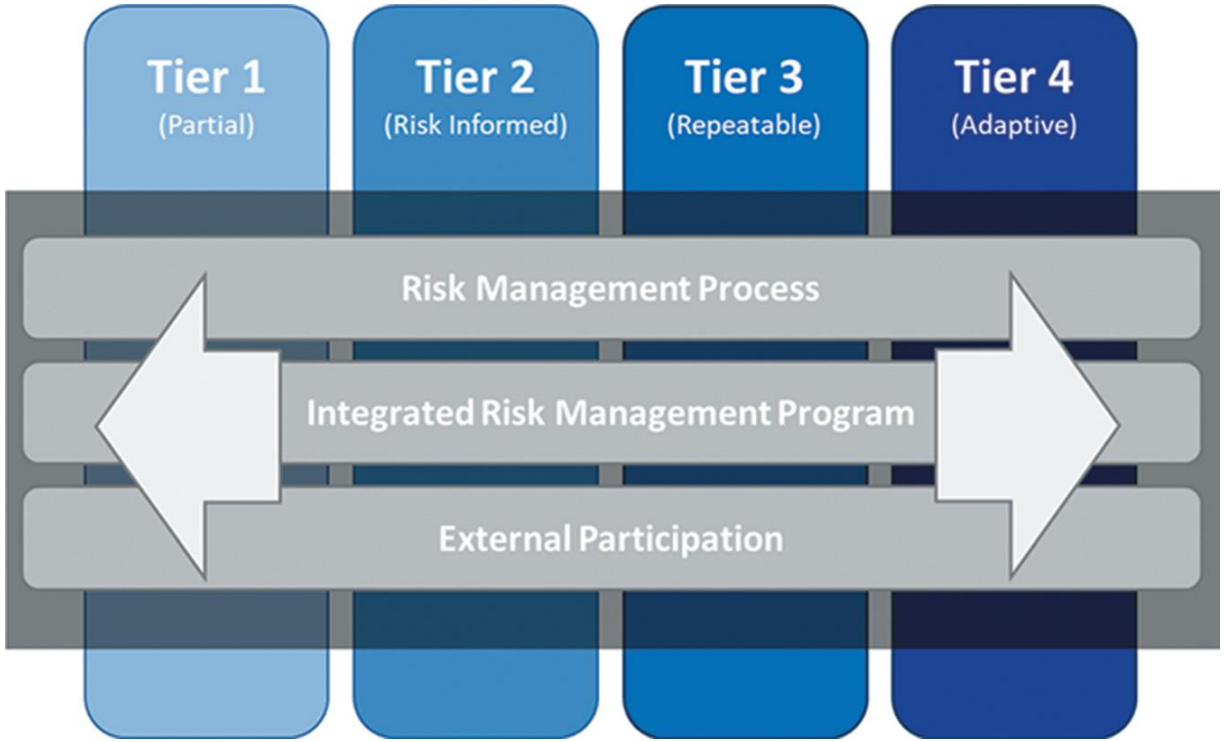
- Dentro de cada uma dessas funções há categorias de atividades, dentro de cada categoria de atividades há subcategorias, e para cada subcategoria há referências informativas.
- A ideia do Framework é que sejam os recursos sejam selecionados a partir de elementos da natureza exclusiva da organização.

Fonte: BRUMFIELD, HAUGLI, 2021

O FRAMEWORK DO NIST

- Os níveis de implementação da estrutura consistem em quatro níveis de **como uma organização vê o risco de segurança cibernética e os processos em vigor para gerenciar esse risco**.
- Cada camada tem o seu nível de maturidade cuja classificação e resume a 4 níveis que são, **Nível 1:** Parcial - o risco é gerenciado de maneira **reativa**, **Nível 2:** Informado sobre riscos – **há práticas de segurança** mas elas **não sao difundidas** para toda a empresa, **Nível 3:** Repetível – **existe a política** publicada na empresa e **Nível 4:** Adaptativo – há adaptação das práticas mediante **as lições aprendidas**.

O FRAMEWORK DO NIST



- Em 2021 a pedido do Governo dos Estados Unidos o **NIST,** foi incitado a fazer uma reformulação da segurança cibernética dos EUA.
- **https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity**

Fonte: BRUMFIELD, HAUGLI, 2021

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.


PUC Minas
Virtual