Centro Universitário - Fundação Escola de Comércio Álvares Penteado (FECAP)
Curso: Análise e Desenvolvimento de Sistemas

Título: Levantamento de Riscos, Vulnerabilidades e Ameaças em Cibersegurança

Aluno: Vinícius Brandão, Murilo Dias, Guilherme Rodrigues e João Henrique Albuquerque
Professor: Ronaldo Araujo
Disciplina: Cibersegurança e Defesa Cibernética

São Paulo - 2025

NIST Cybersecurity Framework Aplicado

1. Identificar (Identify - ID)

1.1 Riscos em Cibersegurança

- **Violação de Dados (Data Breach):** Acesso não autorizado a informações sensíveis dos usuários.
- **Ataques DDoS:** Sobrecarga de servidores, tornando o serviço indisponível.
- **Acesso Não Autorizado:** Invasores obtêm acesso a sistemas críticos.
- **Ataques de Engenharia Social (Phishing):** Indução de usuários a revelar credenciais.
- **Exploração de APIs Inseguras:** Uso de APIs sem proteções adequadas.
- **Riscos Legais e Regulatórios:** Descumprimento de leis e normas de proteção de dados.

1.2 Vulnerabilidades Comuns

- Autenticação fraca (senhas simples, ausência de MFA).
- Softwares desatualizados.
- APIs mal configuradas.
- Criptografia inadequada.
- Gestão de sessão deficiente.
- Infraestrutura insuficiente.

2. Proteger (Protect - PR)

2.1 Medidas de Mitigação

- **Autenticação Multifator (MFA):** Reduz o risco de acesso não autorizado.
- **Criptografia Robusta:** TLS para transmissão, AES-256 para armazenamento.
- **Política de Atualizações:** Correções regulares de software.
- **Hardening de APIs:** Limites de taxa e validação rigorosa.
- **Educação e Treinamento:** Conscientização sobre ameaças sociais.

3. Detectar (Detect - DE)

3.1 Monitoramento e Análise

- **Monitoramento Contínuo:** Registros de logs para detectar comportamentos suspeitos.
- **Testes de Penetração (Pentests):** Identifica e corrige falhas.
- **Análise de Tráfego:** Identifica padrões anormais.

4. Responder (Respond - RS)

4.1 Plano de Resposta a Incidentes

- Procedimentos claros para mitigar ataques.
- Acionamento de equipes de resposta rápida.
- Comunicação eficaz para notificação de partes interessadas.

5. Recuperar (Recover - RC)

5.1 Plano de Recuperação

- **Backups Frequentes:** Redução de impactos de ransomware.
- **Testes de Recuperação:** Avaliação periódica da eficácia das estratégias.
- **Melhoria Contínua:** Aprendizado com incidentes passados.

6. Conclusão

A adoção do NIST Cybersecurity Framework no projeto Sistema de Gestão de Fast And Cheap fortalece a segurança cibernética ao integrar identificação, proteção, detecção, resposta e recuperação. Essas medidas garantem resiliência, proteção de dados e confiança dos usuários.