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

Sumário

---

1. Introdução

Este documento unifica informações relacionadas ao projeto **Sistema de Gestão de *Fast And Cheap*** e conceitos avançados de cibersegurança. O foco é identificar e analisar riscos, vulnerabilidades e ameaças em projetos tecnológicos que envolvem coleta e processamento de dados em plataformas web e aplicativos móveis.

---

2. NIST Cybersecurity Framework Aplicado Identificar (Identify - ID)

Envolve o desenvolvimento de uma compreensão organizacional para gerenciar o risco de segurança cibernética para sistemas, ativos, dados e capacidades.
Objetivo: Desenvolver uma base sólida para o programa de segurança cibernética da organização.
Categorias:

- ID.AM: Gerenciamento de Ativos
- ID.BE: Ambiente de Negócios
- ID.GV: Governança
- ID.RA: Avaliação de Risco
- ID.RM: Estratégia de Gerenciamento de Risco

Riscos em Cibersegurança

- Violação de Dados (Data Breach): Acesso não autorizado a informações sensíveis dos usuários. *Impacto:* Perda de confiança, sanções legais e financeiras.
- Ataques DDoS: Sobrecarga de servidores, tornando o serviço indisponível. *Impacto:* Interrupção do serviço e prejuízos financeiros.
- Acesso Não Autorizado: Invasores obtêm acesso a sistemas críticos. *Impacto:* Comprometimento da integridade do sistema.
- Engenharia Social (Phishing): Induz usuários a revelar credenciais. *Impacto:* Perda de dados e acesso indevido.
- APIs Inseguras: Uso sem proteção adequada. *Impacto:* Exposição de dados e manipulação indevida.
- Riscos Legais e Regulatórios: Descumprimento de leis e normas. *Impacto:* Multas e danos à reputação.

- Concorrência e Baixa Adoção: Baixa aceitação do mercado. *Impacto:* Redução de usuários e retorno financeiro.

Vulnerabilidades Comuns

- Autenticação fraca
- Softwares desatualizados
- APIs mal configuradas
- Criptografia inadequada
- Gestão de sessão deficiente
- Infraestrutura insuficiente

3. Proteger (Protect - PR)

Envolve o desenvolvimento e a implementação de salvaguardas apropriadas para garantir a entrega de serviços críticos.
Objetivo: Implementar controles de segurança para proteger ativos e dados.
Categorias:

- PR.AC: Controle de Acesso
- PR.AT: Conscientização e Treinamento
- PR.DS: Segurança de Dados
- PR.IP: Processos e Procedimentos de Proteção da Informação
- PR.MA: Manutenção
- PR.PT: Tecnologia de Proteção

Medidas de Mitigação

- Autenticação Multifator (MFA)
- Criptografia Robusta (TLS, AES-256)
- Política de Atualizações
- Hardening de APIs
- Educação e Treinamento

4. Detectar (Detect - DE)

Envolve o desenvolvimento e a implementação de atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética.
Objetivo: Identificar rapidamente incidentes de segurança.
Categorias:

- DE.CM: Monitoramento Contínuo de Segurança
- DE.DP: Processos de Detecção

Ameaças Relevantes

- Malware e Ransomware
- Injeção de SQL (SQLi)
- Cross-Site Scripting (XSS)
- Man-in-the-Middle (MitM)
- Ataques de Força Bruta
- Ameaças Humanas e Naturais

5. Responder (Respond - RS)

Envolve o desenvolvimento e a implementação de atividades apropriadas para tomar medidas em relação a um incidente de segurança cibernética detectado.
Objetivo: Minimizar o impacto de incidentes de segurança.
Categorias:

- RS.RP: Planejamento de Resposta
- RS.CO: Comunicação
- RS.AN: Análise
- RS.MI: Mitigação
- RS.IM: Melhorias

Medidas Relacionadas

- Planos de Resposta e Recuperação

6. Recuperar (Recover - RC)

Envolve o desenvolvimento e a implementação de atividades apropriadas para manter planos de resiliência e restaurar quaisquer capacidades ou serviços que foram prejudicados devido a um incidente de segurança cibernética.
Objetivo: Restaurar serviços e capacidades após um incidente.
Categorias:

- RC.RP: Planejamento de Recuperação
- RC.IM: Melhorias
- RC.CO: Comunicação

7. Metodologias Aplicadas

- NIST Cybersecurity Framework
- Matriz GUT (Gravidade, Urgência e Tendência)
- Análise SWOT
- ABNT NBR ISO/IEC 27002

8. Conclusão

A adoção de práticas robustas de cibersegurança é essencial desde o início do projeto Sistema de Gestão de Fast And Cheap. Medidas preventivas, associadas a monitoramento contínuo, garantem resiliência organizacional, proteção de dados sensíveis e confiança dos usuários.