**Cibersegurança e defesa cibernética**

**Nome:** Felipe Ribeiro Almeida

RA: 23024683

Vinícius Miranda Andrade Piovesan

RA: 23025544

Sérgio Ricardo Pedote Junior

RA: 23747441

Matheus de Medeiros Takaki

RA: 23025143

**1. Riscos**

Os riscos representam a possibilidade de um incidente ocorrer devido a vulnerabilidades exploradas por ameaças. Alguns exemplos:

* **Vazamento de dados sensíveis**, comprometendo informações confidenciais.
* **Indisponibilidade do sistema**, impactando operações críticas.
* **Danos financeiros**, resultando em prejuízos diretos e indiretos.
* **Perda de integridade dos dados**, com informações sendo alteradas maliciosamente.
* **Reputação prejudicada**, afetando a credibilidade da organização.

**2. Vulnerabilidades**

Vulnerabilidades são fraquezas no sistema que podem ser exploradas por ameaças. Entre as principais estão:

* **Software desatualizado**, permitindo ataques baseados em exploits conhecidos.
* **Configuração inadequada**, como permissões excessivas e portas abertas desnecessárias.
* **Falta de criptografia**, expondo dados a interceptação.
* **Senhas fracas ou reutilizadas**, facilitando acessos não autorizados.
* **Ausência de segmentação de rede**, permitindo movimentação lateral de invasores.
* **Falta de monitoramento e resposta a incidentes**, aumentando o tempo de detecção e mitigação de ataques.

**3. Ameaças**

As ameaças representam agentes ou técnicas que podem explorar vulnerabilidades. Alguns exemplos comuns incluem:

* **Malware (vírus, worms, ransomware, trojans)**, comprometendo a segurança do sistema.
* **Ataques de phishing**, induzindo usuários a fornecer credenciais ou executar ações perigosas.
* **Ataques de negação de serviço (DDoS)**, tornando sistemas indisponíveis.
* **Exploração de vulnerabilidades (zero-day attacks)**, afetando sistemas sem correções disponíveis.
* **Ataques internos**, causados por funcionários mal-intencionados ou negligentes.
* **Engenharia social**, manipulando pessoas para obter acesso a informações ou sistemas.

**NIST Cybersecurity Framework (CSF)**

**1° Identificar**

Objetivo: Compreender os ativos, riscos e vulnerabilidades do sistema.

* **Inventário de ativos**: Identificar e categorizar dispositivos, softwares e dados críticos.
* **Análise de riscos**: Avaliar ameaças potenciais e impacto nos negócios.
* **Gerenciamento de vulnerabilidades**: Mapear pontos fracos e manter controles de segurança atualizados.
* **Governança**: Estabelecer políticas e regulamentações internas de segurança da informação.

**2° Proteger**

Objetivo: Implementar medidas para minimizar riscos e proteger a infraestrutura.

* **Controle de acesso**: Uso de autenticação multifator (MFA) e privilégios mínimos.
* **Criptografia**: Proteção de dados em repouso e em trânsito.
* **Segurança na rede**: Firewall, segmentação de rede e prevenção contra invasões.
* **Treinamento de usuários**: Conscientização sobre phishing, engenharia social e boas práticas.
* **Gestão de vulnerabilidades**: Aplicação de patches e atualizações regulares.

**3° Detectar**

Objetivo: Identificar atividades suspeitas ou anômalas.

* **Monitoramento contínuo**: Uso de SIEM (Security Information and Event Management) para análise de logs.
* **Detecção de ameaças**: Ferramentas de IDS/IPS (Intrusion Detection/Prevention Systems).
* **Análise de comportamento**: Identificação de acessos incomuns ou tentativas de exploração.

**4° Responder**

Objetivo: Criar planos de resposta para mitigar incidentes de segurança.

* **Plano de resposta a incidentes**: Procedimentos documentados para lidar com ataques.
* **Comunicação**: Notificação de incidentes para partes envolvidas.
* **Análise forense**: Coleta de evidências para entender a origem do ataque.
* **Correção**: Bloqueio de ameaças e implementação de medidas para evitar recorrências.

**5° Recuperar**

Objetivo: Restaurar operações normais após um incidente de segurança.

* **Planos de recuperação**: Estratégias para restaurar sistemas afetados.
* **Backups regulares**: Armazenamento seguro e testes de recuperação de dados.
* **Avaliação pós-incidente**: Aprendizado contínuo para aprimorar a segurança.