Plano de Segurança Digital para o Taboão da Serra Tech Institute (TSTI)

**Resumo Executivo**

O presente plano tem como objetivo desenvolver uma estratégia robusta de segurança digital para o TSTI, enfrentando ameaças complexas e garantindo a integridade dos dados. Utilizando ferramentas como VirusTotal, WiTotal e Nmap, este plano visa:

1. Identificar e analisar ameaças.
2. Monitorar a rede para comportamentos suspeitos.
3. Detectar vulnerabilidades.
4. Mitigar riscos.

**Análise das Ameaças**

1. **Malware**: Análise de arquivos e URLs suspeitos com VirusTotal.
2. **Comportamento anômalo**: Monitoramento de tráfego de rede com Wireshark.
3. **Vulnerabilidades**: Varredura de portas com Nmap.
4. **Exposição de dados**: Proteção contra vazamentos de informações.

**Áreas Impactadas**

1. **Infraestrutura de TI**: Servidores, redes e sistemas.
2. **Dados confidenciais**: Pesquisas, projetos e informações sensíveis.
3. **Comunicação**: E-mails, mensagens instantâneas e videoconferências.
4. **Acesso remoto**: VPNs e acessos externos.

**Ferramentas e Limitações**

1. **VirusTotal**: Análise de malware, mas não substitui soluções antivírus completas.
2. **Wireshark**: Monitoramento de tráfego, mas exige conhecimento técnico.
3. **Nmap**: Varredura de portas, mas pode gerar falso-positivos.

**Implementação**

1. **Análise de riscos**: Identificar vulnerabilidades e ameaças.
2. **Implantação de soluções**: Ferramentas de segurança e treinamento.
3. **Monitoramento contínuo**: Atualizações e ajustes.
4. **Plano de resposta**: Procedimentos em caso de incidentes.

**Desafios**

1. **Conhecimento técnico**: Necessidade de especialização.
2. **Recursos**: Investimento em infraestrutura e ferramentas.
3. **Atualizações**: Manutenção contínua.
4. **Conscientização**: Educação dos usuários.

**Consequências de Inação**

1. **Perda de dados**: Vazamentos ou destruição.
2. **Interrupção de serviços**: Downtime e perda de produtividade.
3. **Danos à reputação**: Confiança e imagem.
4. **Custo financeiro**: Reparação e indenizações.

**Cronograma**

1. **Semana 1-2**: Análise de riscos e planejamento.
2. **Semana 3-4**: Implantação de ferramentas.
3. **Semana 5-8**: Monitoramento e ajustes.
4. **Semana 9-12**: Avaliação e otimização.

**Recursos**

1. **Equipe de TI**: Especialistas em segurança.
2. **Ferramentas**: VirusTotal, Wireshark, Nmap.
3. **Treinamento**: Educação em segurança digital.
4. **Orçamento**: Investimento em infraestrutura.

**Conclusão**

O plano de segurança digital proposto oferece uma abordagem estruturada para proteger o TSTI contra ameaças complexas. Com a implementação dessas medidas, a instituição poderá:

1. Reduzir riscos.
2. Proteger dados confidenciais.
3. Garantir a integridade da infraestrutura.
4. Melhorar a resposta a incidentes.