Planejamento e Estratégia para Coleta de Dados

Objetivo

A entrevista tem o propósito de entender a estrutura de segurança da empresa, identificar boas práticas já adotadas e apontar possíveis melhorias, sem comprometer informações sigilosas ou operacionais sensíveis.

Metodologia

A coleta de dados será realizada por meio de:

1. **Entrevistas estruturadas** com responsáveis pela área de TI e Segurança da Informação.
2. **Formulários eletrônicos** para coletar respostas padronizadas.
3. **Observação in loco** da infraestrutura tecnológica e procedimentos internos.

Roteiro de Entrevista

1. Informações Gerais da Empresa

1. Qual o setor de atuação da empresa?
2. Quantos funcionários trabalham na empresa?
3. A empresa possui uma equipe dedicada à área de TI ou Segurança da Informação?

2. Infraestrutura Tecnológica

4. Quais tipos de dispositivos são utilizados pelos funcionários (desktops, notebooks, tablets, celulares corporativos, etc.)?
5. A empresa possui servidores próprios ou utiliza serviços em nuvem?
6. Existe uma política de atualização de software e sistemas operacionais?

3. Políticas e Procedimentos de Segurança

7. A empresa possui políticas de controle de acesso para sistemas e redes? Se sim, como são implementadas?
8. Existe um processo de gerenciamento de senhas para os funcionários (ex.: troca periódica, requisitos mínimos de senha)?
9. Há uma política de uso de dispositivos pessoais (BYOD - Bring Your Own Device)?

4. Monitoramento e Prevenção de Ameaças

10. São utilizadas ferramentas de monitoramento de segurança, como firewalls, antivírus ou sistemas de detecção de intrusão?
11. Existe alguma prática de auditoria de segurança ou testes de invasão (pentest)?

5. Backup e Recuperação de Dados

12. A empresa realiza backups regulares dos dados? Com que frequência?
13. Há um plano formal de recuperação de desastres em caso de falha ou ataque cibernético?

6. Treinamento e Conscientização

14. Os funcionários recebem treinamentos sobre boas práticas de segurança digital?
15. Há algum programa de conscientização sobre phishing e outros tipos de ataques cibernéticos?

7. Avaliação e Melhorias

16. A empresa já enfrentou algum incidente de segurança? Se sim, como foi resolvido?
17. Há interesse em recomendações para melhorar a segurança da informação?