Avaliação de Risco Baseada no NIST 800-53 (RMF)

Objetivo: Avaliar a postura de segurança cibernética da organização com base no framework NIST 800-53 (RMF).

Público-alvo: Todos os funcionários da empresa.

Perguntas:

1. Controle de Acesso

- **1.1** O acesso aos sistemas e dados da organização é controlado por meio de autenticação e autorização?
- **1.2** As senhas são fortes e complexas?
- **1.3** O acesso aos sistemas e dados é revogado quando não é mais necessário?

2. Conscientização e Treinamento em Segurança

- **2.1** Os funcionários são treinados em segurança cibernética?
- **2.2** O treinamento abrange tópicos como phishing, malware e engenharia social?
- **2.3** Os funcionários são incentivados a relatar incidentes de segurança?

3. Gestão de Riscos

- **3.1** A organização realiza avaliações de risco regularmente?
- **3.2** Os riscos de segurança cibernética são identificados, avaliados e priorizados?
- **3.3** São implementados planos de ação para mitigar os riscos de segurança cibernética?

4. Segurança de Rede

- **4.1** A rede da organização é protegida por firewalls e outros dispositivos de segurança?
- **4.2** O acesso à rede Wi-Fi é seguro?
- **4.3** As atualizações de software são instaladas regularmente?

5. Segurança de Software

- **5.1** O software utilizado pela organização é licenciado e autenticado?
- **5.2** O software é atualizado regularmente com patches de segurança?
- **5.3** O software é desenvolvido e testado com segurança em mente?

6. Segurança de Hardware

- **6.1** Os dispositivos de hardware da organização são armazenados em local seguro?
- **6.2** Os dispositivos de hardware são criptografados?
- **6.3** O firmware dos dispositivos de hardware é atualizado regularmente?

7. Incidentes de Segurança

- **7.1** A organização possui um plano de resposta a incidentes de segurança?
- **7.2** Os incidentes de segurança são registrados e investigados?
- **7.3** São tomadas medidas para evitar que incidentes de segurança semelhantes ocorram no futuro?

8. Continuidade de Negócios e Recuperação de Desastres

- **8.1** A organização possui um plano de continuidade de negócios?

- **8.2** O plano de continuidade de negócios é testado regularmente?
- **8.3** A organização possui um plano de recuperação de desastres?

9. Conformidade

- **9.1** A organização está em conformidade com as leis e regulamentos relevantes de segurança cibernética?
- **9.2** A organização possui uma política de segurança cibernética documentada?
- **9.3** A política de segurança cibernética é revisada e atualizada regularmente?

10. Melhoria Contínua

- **10.1** A organização realiza avaliações regulares da postura de segurança cibernética?
- **10.2** São implementadas medidas para melhorar a postura de segurança cibernética da organização?
- **10.3** A cultura da organização promove a segurança cibernética?

Observações:

- Esta auto auditoria é apenas um ponto de partida.
- É recomendável que a organização realize uma avaliação de segurança mais abrangente por um profissional qualificado.