**🔒 1. Gestão de Riscos de Segurança da Informação**

**O que é?**

É um **processo contínuo e estruturado** que visa **identificar, avaliar, mitigar e monitorar** os riscos que podem afetar os ativos de informação de uma organização.

**Etapas detalhadas:**

**a) Identificação de Riscos**

* **Identificação de ativos**: Quais são os dados, sistemas, redes e infraestruturas críticas?
* **Ameaças**: O que pode causar danos? (ex: hackers, malware, erro humano)
* **Vulnerabilidades**: Fraquezas que podem ser exploradas (ex: software desatualizado, senhas fracas)

**b) Avaliação de Riscos**

* **Impacto**: Qual o prejuízo se o risco se concretizar? (financeiro, reputação, operacional)
* **Probabilidade**: Qual a chance de o risco ocorrer?
* **Classificação**: Risco alto, médio ou baixo.

**c) Mitigação de Riscos**

* Implementar **controles de segurança**: firewalls, antivírus, criptografia, políticas de acesso.
* Elaborar **planos de resposta a incidentes**.

**d) Monitoramento e Revisão**

* Acompanhamento contínuo dos riscos.
* Reavaliação periódica para ajustar medidas.

**🚨 2. Resposta a Incidentes de Segurança**

**O que é?**

É uma **abordagem organizada** para lidar com violações de segurança, com o objetivo de **minimizar danos**, **restaurar sistemas** e **evitar repetição**.

**Etapas detalhadas:**

**a) Preparação**

* Ter um **plano de resposta** documentado.
* Treinar equipes.
* Ter ferramentas de detecção e resposta.

**b) Detecção e Análise**

* Identificar o incidente.
* Coletar evidências (logs, arquivos, etc.).
* Classificar o incidente (gravidade, tipo, urgência).

**c) Contenção e Neutralização**

* Isolar sistemas afetados.
* Remover malware ou bloquear acessos não autorizados.

**d) Recuperação**

* Restaurar sistemas a partir de backups.
* Verificar se não há mais ameaças.

**e) Lições Aprendidas**

* Analisar o que aconteceu e como foi resolvido.
* Melhorar processos e políticas.

**📊 3. Classificação de Incidentes**

**Critérios:**

**a) Por Gravidade**

* **Alto**: Paralisação crítica, vazamento massivo de dados.
* **Médio**: Afeta parte da operação.
* **Baixo**: Impacto localizado, fácil contenção.

**b) Por Tipo**

* **Malware**: vírus, ransomware, worms.
* **Phishing**: golpe por e-mail ou mensagem.
* **DDoS**: ataque de negação de serviço.
* **Vazamento de dados**: exposição não autorizada de informações.

**c) Por Urgência**

* **Imediata**: Requer ação agora.
* **Urgente**: Deve ser resolvido em horas.
* **Regular**: Pode ser programado.

**d) Por Complexidade**

* **Simples**: Poucos sistemas afetados, fácil resolução.
* **Complexo**: Múltiplos sistemas, requer equipe especializada.

**⚖️ 4. LGPD (Lei Geral de Proteção de Dados Pessoais)**

**O que diz?**

A LGPD exige que empresas:

* Protejam dados pessoais.
* Notifiquem incidentes à autoridade (ANPD) e aos afetados.
* Adotem medidas de segurança adequadas.

**Multas e Advertências:**

* **Advertência**: para casos leves ou primeira ocorrência.
* **Multa**: até 2% do faturamento, limitada a R$ 50 milhões por infração.
* **Fatores que influenciam**:
  + Existência de um programa de segurança.
  + Rapidez na resposta.
  + Transparência com afetados.
  + Cooperação com autoridades.

**Ter um plano de gestão de riscos:**

* **Não impede multas**, mas **reduz a chance** e pode **atenuar a pena**.
* Mostra que a empresa agiu com **diligência**.

**🧩 5. Exemplos de Casos Reais**

**a) Colonial Pipeline (Ransomware)**

* Pagou resgate de US$ 4,4 milhões.
* Paralisou operações por dias.
* Falha em: controle de acesso, backup, treinamento.

**b) Equifax (Vazamento de Dados)**

* Exposição de dados de 145 milhões de pessoas.
* Falha em: atualização de sistemas, gestão de vulnerabilidades.

**c) Google (Ataque DDoS)**

* Maior ataque de negação de serviço da história (2,56 Tbps).
* Mitigou com absorção de tráfego e roteamento inteligente.