



Governança e Risco da Segurança

Como gerenciar a Segurança?



- Dentro da empresa, a área de Segurança da Informação, precisa ter um planejamento estratégico.
- A direção da empresa, determina o destino da organização e a área de segurança tem que avaliar o impacto e definir o roadmap.
- Tudo isso vai para a Governança de Segurança

O que é Governança?

- Ato de governar, liderar
- Define o planejamento estratégico
- Time define e coordena outras áreas



Planejamento da Segurança



- Medir os gaps
- Definir o plano e/ou projetos
- Executar os projetos
- Monitorar as demandas

Gestão de Risco



- Risco é a chance de algo acontecer
- Medir o impacto nos negócios e a chance de acontecer
- Quanto mais alto o impacto ou a chance, muda a classificação
- Risco Baixo, Médio e Alto
- Exemplo: Risco de perda de arquivos, risco de acesso não autorizado

Identificação de Ativos



Ativo é algo que tem potencial de gerar receita para a empresa.

Exemplos:

- Clientes
- Funcionários
- Fórmulas de produtos
- Bases de dados
- Sistemas
- Equipamentos

Identificação de Riscos



Para identificar riscos, você precisará de conhecimento de negócio

Avaliar o ciclo de vida do ativo

Avaliar o uso do ativo

Consultar um especialista

Definição de Controles



- Uma vez identificado o risco, deve-se estabelecer um controle de segurança
- O controle pode ser um processo ou uma ferramenta

Exemplos:

- Crachá para acesso a empresa
- Senha para abrir o computador
- Firewall e Antivírus

Monitoramento de Risco



- Devemos olhar por toda a tecnologia, em busca de problemas
- Monitoramento em tempo real e passivo através dos logs
- Busca por atividades suspeitas, falhas no processo, disponibilidade



Resumo

- O que é Governança
- Planejamento da Segurança
- Gestão de Risco
- Identificação de Ativos
- Identificação de Riscos
- Definição de Controles
- Monitoramento de Risco



Adequando às leis

Como as leis influenciam a área de segurança?