1.Security considerations

Profissionais de segurança de TI precisam estar atentos às **regulamentações** que afetam suas organizações e os tipos de dados coletados. Isso inclui não apenas as informações armazenadas em aplicativos, mas também **arquivos de log** gerados por sistemas. Algumas organizações são obrigadas a **reter certos tipos de dados por longos períodos**, como e-mails corporativos, que podem precisar ser armazenados por anos e acessados sob demanda.

Uma das regulamentações mais conhecidas é a **Sarbanes-Oxley Act (SOX)**, oficialmente chamada de **Public Company Accounting Reform and Investor Protection Act of 2002**. Essa lei foca na transparência das informações financeiras das empresas, exigindo proteção rigorosa dos dados contábeis e garantindo que apenas indivíduos autorizados tenham acesso a essas informações.

Na área da saúde, há a **HIPAA (Health Insurance Portability and Accountability Act)**, que protege os dados médicos dos pacientes. Essa lei regula não apenas o **armazenamento** das informações, mas também a **transmissão e divulgação** para terceiros.

Questões **legais** também fazem parte do trabalho dos profissionais de segurança. Por isso, é essencial que as organizações tenham **processos formais para relatar atividades ilegais**. Além disso, quando há um **pedido de retenção legal (legal hold)**, **a equipe de TI deve garantir que os dados fiquem armazenados e disponíveis para futuras investigações**.

Muitos países possuem leis que **exigem a divulgação de violações de segurança**. Se uma empresa sofre um vazamento de dados, pode ser legalmente obrigada a informar clientes e autoridades dentro de um prazo específico. Como essas regras variam de acordo com a localização, as empresas precisam seguir os regulamentos específicos de cada região onde atuam.

A computação em **nuvem** trouxe desafios adicionais do ponto de vista legal. Como dados e aplicações podem ser distribuídos globalmente, algumas leis determinam que **as informações de cidadãos devem ser armazenadas dentro do próprio país**. Isso exige que empresas gerenciem cuidadosamente onde seus servidores estão localizados para garantir conformidade com as regras de proteção de dados.

Diferentes setores também possuem **requisitos específicos de segurança**. No setor de **energia e infraestrutura crítica**, por exemplo, muitas redes são **isoladas fisicamente** (*air-gapped*) para evitar ataques cibernéticos. Já na área da **saúde**, onde os dados precisam ser acessíveis a profissionais médicos, são adotadas **criptografia avançada e mecanismos rigorosos de controle de acesso** para garantir a privacidade das informações.

O nível de **segurança** também varia conforme o **escopo da organização**. Governos **locais e regionais** lidam principalmente com dados administrativos e registros públicos, enquanto governos **nacionais** precisam proteger informações mais sensíveis, como dados de defesa. Já **empresas globais** enfrentam desafios adicionais, pois operam em múltiplas jurisdições, cada uma com suas próprias leis de proteção de dados. Isso torna a **conformidade regulatória** um aspecto crítico para a segurança corporativa em escala mundial.