1.Security policies

Um dos principais objetivos de um administrador de segurança é garantir a **Confidencialidade, Integridade e Disponibilidade** dos dados, um conceito conhecido como **CIA**. Para atingir essa meta, é essencial definir políticas e regras que todos devem seguir para manter a segurança dos sistemas e informações. Essas políticas podem ser amplas, estabelecendo requisitos gerais de armazenamento de dados e procedimentos de resposta a incidentes, ou específicas, detalhando o uso da rede Wi-Fi e os requisitos para acesso remoto.

A maioria das organizações mantém um conjunto de **políticas de segurança da informação, documentando diretrizes essenciais para a proteção da infraestrutura de TI**. Em muitos casos, essas políticas não são apenas recomendações, mas exigências obrigatórias para manter a conformidade com normas e regulamentos. Além de proteger a organização, as políticas de segurança ajudam a responder a questões como: o que fazer ao detectar um vírus em um computador, quais procedimentos seguir para conexão via VPN e como lidar com uma vulnerabilidade explorada por um atacante.

Além disso, essas políticas definem claramente **papéis e responsabilidades**, especificando quem deve ser contatado em caso de dúvidas ou emergências de segurança. No entanto, ter diretrizes escritas não é suficiente; a organização deve garantir sua **implementação e fiscalização**.

Uma política fundamental dentro das organizações é a **Política de Uso Aceitável** (***Acceptable Use Policy*** **- AUP**), **que define o que os funcionários podem e não podem fazer com os dispositivos corporativos**, como computadores, telefones e redes. Essa política não apenas orienta os usuários, mas também protege a empresa contra responsabilidade legal. Se um funcionário violar essas regras e for demitido, a organização terá documentação para justificar a decisão.

Além da segurança operacional, as empresas precisam se preparar para falhas imprevistas. **Planos de Continuidade de Negócios** (***Business Continuity Plans*** **- BCP**) **estabelecem procedimentos para garantir que a empresa continue funcionando mesmo diante de problemas técnicos**. Por exemplo, se uma rede de processamento de cartões de crédito falhar, o plano pode instruir os funcionários a realizarem transações manualmente e confirmá-las via telefone. Esses planos devem ser testados e atualizados regularmente para garantir sua eficácia.

Se uma interrupção afetar um grande número de pessoas ou durar muito tempo, entra em ação o **Plano de Recuperação de Desastres** (*Disaster Recovery Plan* - DRP). **Esse plano cobre cenários como desastres naturais (furacões, inundações), falhas sistêmicas ou ataques cibernéticos, garantindo que a organização tenha procedimentos claros para retomar as operações**. Um DRP pode incluir estratégias

como locais alternativos de trabalho, backups de dados e restauração de sistemas críticos.

A resposta a incidentes de segurança também deve ser bem planejada. Se um funcionário acidentalmente executar um malware a partir de um anexo de e-mail, por exemplo, a empresa precisa ter uma política que oriente os próximos passos. Isso se aplica a diversos cenários, como ataques **DDoS**, vazamentos de dados e exploração de vulnerabilidades.

Para lidar com esses desafios, as organizações contam com **equipes de resposta a incidentes**, compostas por diferentes profissionais, como especialistas em segurança, gerentes de TI, oficiais de conformidade e funcionários técnicos. A equipe deve seguir diretrizes estabelecidas pelo **NIST Special Publication 800-61 Revision 2**, que define um ciclo de resposta incluindo **preparação, detecção, contenção, erradicação, recuperação e atividades pós-incidente**.

Outra política essencial para empresas que desenvolvem software é o **Ciclo de Vida do Desenvolvimento de Software** (*Software Development Lifecycle* - SDLC). **Ele define um processo estruturado para criação de aplicativos, incluindo levantamento de requisitos, desenvolvimento, testes e implementação**. Dois modelos comuns são o **Waterfall**, um processo linear onde cada fase é concluída antes da próxima, e o **Agile**, que permite entregas contínuas e aprimoramentos constantes.

Por fim, **gerenciamento de mudanças** é um componente crítico da segurança organizacional. Qualquer alteração em um sistema, como atualização de software, modificação de configurações de firewall ou ajustes em um servidor, deve seguir um processo formal para minimizar riscos. Empresas bem estruturadas realizam reuniões regulares para planejar mudanças e documentar seus impactos, garantindo que qualquer alteração possa ser revertida se necessário.

A implementação de políticas de segurança e gestão de riscos permite que as organizações se protejam contra ameaças cibernéticas e estejam preparadas para responder de forma eficaz a incidentes, assegurando a continuidade dos negócios e a integridade dos dados.