1.Security procedures

Um dos procedimentos mais comuns em segurança dentro de qualquer organização é o **gerenciamento de mudanças**. **Esse processo garante que toda alteração em sistemas siga um conjunto estruturado de diretrizes, evitando falhas, confusões e erros**. O gerenciamento de mudanças envolve várias etapas, começando pela definição do escopo da alteração. Isso pode incluir desde a modificação de um único servidor até a atualização de múltiplos dispositivos ou sistemas operacionais inteiros. Também é essencial avaliar os riscos associados à mudança e documentar um plano detalhado do que será alterado.

A maioria das empresas possui um **Conselho de Controle de Mudanças** (***Change Control Board***), que analisa todas as solicitações de alteração, aprova e agenda sua implementação. Esse conselho também verifica a existência de **planos de contingência**, garantindo que, caso algo dê errado, seja possível reverter a mudança sem impactos significativos. Após a implementação, todas as modificações devem ser registradas para que a equipe de segurança e TI saiba exatamente o que foi alterado.

Outro processo essencial é o **onboarding**, que trata da integração de novos funcionários à organização. **Durante esse processo, a equipe de segurança fornece ao novo colaborador documentos como o manual do funcionário e a política de uso aceitável, que precisam ser assinados e aceitos**. Contas de usuário são criadas para permitir o acesso à rede, e permissões específicas são configuradas de acordo com o cargo. Além disso, o funcionário recebe dispositivos como laptops e celulares corporativos para desempenhar suas funções.

Da mesma forma, existe o **offboarding**, **que assegura que todas as credenciais e acessos sejam removidos quando um funcionário deixa a organização**. Esse processo define o que deve ser feito com os equipamentos fornecidos ao colaborador e os dados armazenados em seus dispositivos. Como boa prática, a conta do usuário não deve ser deletada imediatamente, pois pode conter **arquivos criptografados** ou informações importantes que ainda precisam ser acessadas. A remoção de contas deve ser feita de maneira planejada para evitar perdas irreversíveis.

Organizações frequentemente utilizam **playbooks** para definir as etapas a serem seguidas em diferentes cenários. **Um playbook fornece um guia passo a passo para lidar com incidentes, como vazamentos de dados ou ataques de ransomware**. Cada tipo de incidente possui um playbook específico, garantindo que a equipe saiba exatamente o que fazer e em qual ordem.

Esses processos podem ser otimizados com plataformas **SOAR** (*Security Orchestration, Automation, and Response*), **que integram diferentes soluções de segurança e permitem a automação de tarefas repetitivas**. Com SOAR, atividades como bloqueio de usuários suspeitos e análise de tráfego malicioso podem ser

automatizadas, permitindo que a equipe de segurança foque em incidentes mais complexos.

O monitoramento contínuo das políticas e processos é essencial para manter a segurança da organização. Isso pode envolver a revisão de **playbooks**, a aquisição de novas tecnologias e a adaptação a novas ameaças emergentes. Como os atacantes estão sempre desenvolvendo novas técnicas, a segurança deve ser constantemente ajustada para mitigar riscos.

A estrutura de governança nas organizações geralmente começa com um **conselho**, que pode ser um **conselho de administração** ou um grupo de especialistas que define diretrizes estratégicas. As decisões do conselho são implementadas por comitês especializados, compostos por especialistas em segurança, TI e conformidade.

No setor público, o processo de governança pode envolver questões legais, administrativas e políticas, sendo mais transparente e acessível ao público. Tanto no setor privado quanto no público, a governança pode ser **centralizada**, **onde um único grupo toma decisões para toda a organização**, ou **descentralizada**, **permitindo que equipes individuais tomem decisões baseadas em suas necessidades**. O modelo ideal depende da estrutura e dos objetivos da organização.