Objetivo: Os alunos do grupo devem se colocar no papel de consultores de segurança e criar um conjunto básico de políticas de segurança da informação para uma pequena empresa fictícia composto por:

- **Políticas de acesso e controle de usuários;**

As políticas de acesso e controle de usuários são um conjunto de regras que definem se um usuário tem permissão para acessar um recurso protegido. O objetivo é garantir a segurança das informações, impedindo acessos não autorizados.

Diretrizes:

- Identificar os grupos de usuários da empresa e definir qual o nível de acesso baseado no cargo;

- Implementar processos de autenticação, como por exemplo, autenticação multifator (MFA) ou autenticação de dois fatores (2FA);

- Revisar e atualizar a política de forma contínua;

- Sistema de acesso por senha;

- Estipular um limite de tempo para uma senha. Exemplo: a cada 90 dias.
-

As políticas citadas são importantes porque implementam a segurança da informação, prevenindo que os dados sejam roubados e vazados. Também define que cada usuário tem unicamente uma responsabilidade, permitindo que a empresa tenha uma visão ampla das funcionalidades dos trabalhadores.

- **Política de uso de dispositivos móveis e redes;**

Uma política de uso de dispositivos móveis e redes deve estabelecer diretrizes para o uso de dispositivos móveis e a segurança da informação, de modo a proteger os dados e evitar perdas.

Diretrizes:

- Definir se é permitido pela empresa o uso de dispositivos pessoais ou apenas corporativos.

- Realizar treinamentos periódicos para que os colaboradores possam reconhecer possíveis incidentes.

- Obrigar os usuários a manterem sigilo e protegerem as informações confidenciais.

- Proibir o compartilhamento de dispositivos com pessoas que não sejam da empresa.

- Todos os incidentes devem ser comunicados ao departamento de TI em um prazo de 24 horas.

- A equipe de TI deve fazer uma análise e contenção e conter o incidente em até 48 horas.

Com a crescente adoção do trabalho remoto e o uso de dispositivos móveis, é fundamental criar normas que assegurem a proteção dos dados em movimento e aqueles armazenados fora do ambiente da empresa.

- **Diretrizes para resposta a incidentes de segurança;**

    - Estabelecer uma norma para a reação de incidentes, assim como designando uma equipe para exercer a função;

    - Documentar e estabelecer métricas de segurança que indicam, por exemplo, como e quando aconteceu o ataque, para assim melhorar a qualidade de segurança da empresa;

    - Formar uma equipe dedicada à identificar e relatar incidentes;

As diretrizes implantadas reforçam a empresa, minimizando os danos que podem ser causados à ela. Também é importante por estar de acordo com os padrões de segurança estabelecidos pela ISO, por exemplo.

- **Política de backup e recuperação de desastres.**

Diretrizes:

- É necessário ter uma frequência de backups. Deve ser efetuado, pelo menos, um backup por dia.

- Os backups necessitam de um lugar seguro para serem armazenados, de preferência, fora do local físico da empresa, prevenindo incidentes naturais.

- Os backups devem ser testados semestralmente a fim de garantir a eficiência do plano.

- A documentação do plano de desastres deve ser acessível a todos os envolvidos no processo para que possa ser usada posteriormente.

Uma política de backup é essencial para qualquer empresa que tenha informações ativas nas quais sejam necessárias serem armazenadas de maneira confidencial, pois ela permite que as informações, mesmo que sofram algum ataque ou perda, sejam recuperadas de modo seguro.