

Atividade 1.

1. Políticas de Acesso e Controle de Usuários

Políticas Propostas

- **Autenticação de Usuários:** Todos os funcionários devem usar senhas fortes e únicas.
- **Revisão de Acesso:** As permissões de acesso devem ser revisadas mensalmente para garantir que apenas os usuários autorizados mantenham o acesso.

Justificativa

Essas medidas ajudam a diminuir o risco de acessos não autorizados por pessoas de fora da organização e garantem que os dados sensíveis sejam acessados apenas por usuários que realmente necessitam.

2. Política de Uso de Dispositivos Móveis e Redes

Políticas Propostas

- **Uso de Dispositivos Móveis:** Os funcionários devem usar apenas dispositivos autorizados para acessar informações da empresa. Dispositivos pessoais podem ser utilizados apenas sob condições pontuais e monitoradas.
- **Proibição de Redes Públicas:** O uso de redes Wi-Fi públicas para acessar dados da empresa é proibido, a menos que uma VPN autorizado pela organização esteja em uso.

Justificativa

Essas políticas garantem que os dados da empresa permaneçam protegidos, mesmo quando acessados fora do ambiente corporativo.

3. Diretrizes para Resposta a Incidentes de Segurança

Políticas Propostas

- **Identificação de Incidentes:** Todos os colaboradores devem ser treinados para identificar e relatar incidentes de segurança imediatamente.
- **Equipes de Resposta a Incidentes:** Contratar uma empresa especializada em consultoria de segurança da informação para responder rapidamente a incidentes de segurança.

Justificativa

Uma resposta rápida e organizada é fundamental para limitar o impacto dos incidentes e proteger a integridade dos dados da empresa.

4. Política de Backup e Recuperação de Desastres

Políticas Propostas

- **Armazenamento Seguro:** Os backups devem ser armazenados em local seguro, com uma cópia off-site para proteger contra desastres locais.
- **Teste de Recuperação:** Recuperações de backup devem ser testadas trimestralmente para garantir a eficácia do plano.

Justificativa

Um bom plano de backup e recuperação é essencial para garantir a continuidade dos negócios e a integridade dos dados, minimizando o impacto de falhas ou desastres.