**DESENVOLVIMENTO DE POLÍTICAS DE SEGURANÇA PARA UMA PEQUENA EMPRESA;**

1. Política de acesso a usuários:

* Controle de atualização de senha trimestral;
  + Prevenção a senhas fracas e desatualizadas;
* Autenticação de múltiplos fatores;
  + Dificulta o acesso não autorizado aos sistemas da empresa;
* Revisão de acessos;
  + Analisa os acessos indesejados durante o período.

1. Política de uso de dispositivos móveis e redes

* Uso de VPN:
  + Uso de VPN para acessar a rede coorporativa garantido a integridade dos dados;
* Proteção dos dispositivos:
  + Restrição a sites com baixa segurança;
* Proibição de acesso a redes públicas;
  + Ao bloquear o acesso a redes públicas, é possível diminuir os riscos de invasão, impedindo o usuário de se conectar em redes de baixa segurança.

1. Diretrizes para respostas a incidentes de segurança:

* Bloqueio de acesso:
  + Após várias tentativas falhas, o acesso ao sistema é bloqueado, sendo liberado somente pela administração;
* Treinamento regular;
  + Treinamentos regulares aos usuários para não clicarem em links maliciosos ou visitarem sites suspeitos;
* Uso de antivírus;
  + O antivírus instalado impede que arquivos maliciosos sejam executados e danifiquem o computador;

1. Políticas de backup e recuperação de dados;

* Backup físico regular:
  + Realização de backup físico constante para evitar perdas de dados em casos de sequestro.
* Backup em nuvem:
  + Garantir que haja uma cópia dos arquivos em nuvem em caso de perda de informação;
* Criptografia de backups;
  + Garantir que, caso alguém roube os dados, não conseguirá decifrar as informações nele contidas.