\*\*Políticas de Segurança da Informação para uma Pequena Empresa Fictícia\*\*

1. Políticas de Acesso e Controle de Usuários:

- Princípio do Menor Privilégio: Atribuir aos usuários apenas os acessos necessários para desempenharem suas funções. Os privilégios devem ser revistos periodicamente.

- Autenticação Forte: Todos os acessos ao sistema devem ser protegidos por autenticação multifatorial (MFA), especialmente para sistemas críticos.

Gerenciamento de Senhas: As senhas devem ser complexas, com pelo menos 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos.

Controle de Acessos Baseado em Funções (RBAC): Atribuir acessos com base nas funções desempenhadas pelo colaborador, com a possibilidade de revogação imediata quando o colaborador mudar de função ou for desligado da empresa.

-

Uso Responsável de Dispositivos Móveis: Dispositivos móveis corporativos devem ser configurados com senhas fortes, criptografia e bloqueio automático de tela após 5 minutos de inatividade.

-

VPN (Rede Privada Virtual): Para acesso remoto aos sistemas da empresa, é obrigatória a utilização de uma VPN segura, garantindo que a comunicação entre o dispositivo e a rede da empresa seja criptografada.

-

Erda ou Roubo de Dispositivo: Em caso de perda ou roubo de um dispositivo corporativo, o usuário deve informar imediatamente ao departamento de TI, que tomará as medidas necessárias, como o bloqueio remoto e a limpeza dos dados do dispositivo.

3.

Definição de Incidente de Segurança: Qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade das informações da empresa, como ataques cibernéticos, vazamento de dados ou falhas em sistemas críticos.

-

Treinamento Regular: Todos os colaboradores devem ser treinados anualmente sobre como identificar e responder a incidentes de segurança, incluindo phishing e engenharia social.

-

Registro e Análise Pós-Incidente: Após a resolução do incidente, um relatório deve ser gerado, detalhando as causas, ações tomadas e medidas preventivas para evitar futuros incidentes semelhantes.

4.

Backup Regular: Todos os dados críticos devem ser respaldados diariamente, com armazenamento em pelo menos duas localizações distintas (por exemplo, um backup local e na nuvem).

-

Testes de Recuperação: A recuperação dos backups deve ser testada trimestralmente para garantir que os dados possam ser restaurados de forma eficiente e sem falhas.

-

Plano de Recuperação de Desastres (DRP): A empresa deve ter um plano documentado e testado para restaurar operações em caso de falhas catastróficas (ex: incêndios, falhas de hardware, ataques de ransomware).

Retenção de Backups: Os backups devem ser armazenados por um período mínimo de 30 dias e apagados de forma segura após esse período.

Essas Políticas devem ser revisadas e atualizadas periodicamente, garantindo que acompanhem as mudanças nas tecnologias e nas necessidades de segurança da empresa.