Políticas de segurança da informação

para uma uma empresa de pequeno porte

Douglas Evangelista - 82516629

Emilly dos santos ferreira - 825153657

Henrique Lima Cândido - 825156385

Larissa Oliveira dos Santos - 82516871

Rafael Gomes Taiar - 825113488

Rafaela Maria da Silva - 825134501

Introdução

A segurança da informação é essencial para empresas de todos os portes, inclusive as pequenas, que muitas vezes são mais vulneráveis por falta de políticas adequadas. Como consultores especializados na área, desenvolvemos diretrizes fundamentais que visam proteger os dados da organização, garantir a integridade de seus sistemas e estabelecer boas práticas entre seus colaboradores.

O objetivo é oferecer um material claro, objetivo e aplicável, que possa servir como base para a estruturação de uma cultura de segurança eficaz dentro da empresa, alinhada às necessidades e limitações típicas de negócios de menor porte.

Políticas de acesso e controle de usuários

1. Identificação e Autenticação: Cada usuário deve possuir um identificador único. Implementar autenticação multifator (MFA) para sistemas críticos,adicionando uma camada extra de segurança.

2. Princípio do Menor Privilégio: Conceder aos usuários apenas as permissões necessárias para desempenhar suas funções, minimizando riscos de acessos indevidos.

3. Gestão de Contas: Criar contas mediante solicitação formal e aprovação do gestor; realizar revisões periódicas dos acessos concedidos; desativar imediatamente contas de usuários desligados.

4. Política de Senhas: Exigir senhas complexas, com no mínimo 12 caracteres, incluindo letras maiúsculas, minúsculas, números e caracteres especiais; recomendar a troca de senhas a cada 90 dias; proibir o armazenamento de senhas em locais não seguros.

5. Monitoramento: Implementar sistemas de monitoramento para registrar e analisar atividades de acesso, identificando comportamentos anômalos.

6. Acesso de Terceiros: Exigir termos de confidencialidade assinados por terceiros; conceder acessos temporários e restritos ao necessário; monitorar atividades de terceiros durante o período de acesso.

7. Treinamento e Conscientização: Realizar treinamentos periódicos sobre políticas de segurança da informação, destacando a importância do controle de acessos.

Política de uso de dispositivos móveis e redes

1. Proteção de Acesso: Dispositivos móveis corporativos devem ser protegidos por senha, biometria ou reconhecimento facial.

2. Instalação de Aplicativos: É proibido instalar aplicativos não autorizados em dispositivos corporativos. Apenas softwares aprovados pela empresa poderão ser utilizados.

3. Conexão de Rede: O uso de Wi-Fi público para acesso a dados corporativos deve ser evitado. Se necessário, deve-se utilizar VPN corporativa para garantir a segurança da conexão.

4. Atualizações e Segurança: Todos os dispositivos móveis devem estar sempre atualizados com as versões mais recentes dos sistemas operacionais e aplicativos. Além disso, devem possuir antivírus ativos.

5. Serviços de Nuvem: É proibida a sincronização de dados corporativos com serviços de nuvem pessoais, como Google Drive, Dropbox, OneDrive pessoal, entre outros. Apenas soluções corporativas autorizadas poderão ser utilizadas para esse fim.

Diretrizes para resposta a incidentes de segurança

1. Classificação de Incidentes: Os incidentes de segurança devem ser classificados em categorias, para cada categoria terá um nível de resposta e prioridade.

2. Notificação e Comunicação: Todos os colaboradores devem receber treinamento para reconhecer e relatar incidentes; deve ser feito um relatório detalhando o ocorrido; se houver risco real de exposição de dados, a empresa deve comunicar com usuários afetados, clientes ou órgãos reguladores de forma transparente.

3. Processo de Resposta: Detecção de registro do incidente; impedir o avanço ou impacto maior; remover a causa raiz; restaurar sistemas e dados afetados com backup seguro; análise pós-incidente para gerar ações preventivas futuras.

Política de backup e recuperação de desastres

1. Frequência: Os Backups devem ser realizados diariamente para todos os dados críticos, bancos de dados, arquivos compartilhados e configurações de sistemas essenciais.

2. Armazenamento: Os backups devem ser armazenados de duas formas, em um servidor local protegido fisicamente e em Nuvem.

3. Acesso aos Backups: O acesso aos arquivos de backup será restrito a pessoal autorizado da área de TI; todos os acessos devem ser registrados e auditáveis.

4. Plano de Recuperação de Desastres: A empresa manterá um Plano de Recuperação de Desastres documentado; este plano deve conter contatos de emergência, procedimentos de restauração de sistemas, estimativa de tempo de recuperação e tolerância à perda de dados; este plano deve ser revisado anualmente.

Obrigado pela atenção!

Professor Calvetti- UC Sistemas Computacionais e Segurança
Universidade São Judas Tadeu