Políticas de Segurança da Informação para Pequenas Empresas

Grupo: Bruno Rodrigues Reis RA: 8222243147

Marcello Andrade Rodrigues dos Santos RA: 824216008

Jullia Roberta de Oliveira Marcolino RA: 825162649

William Fernandes Trindade RA: 824216629

Ryan Rocha Pereira RA: 825155072

Referência às Normas ISO: As políticas propostas seguem as diretrizes das normas internacionais da família **ISO/IEC 27000**, com destaque para:

- **ISO/IEC 27001** – Requisitos para um Sistema de Gestão de Segurança da Informação (SGSI);
- **ISO/IEC 27002** – Código de prática para controles de segurança da informação;
- **ISO/IEC 27005** – Diretrizes para gestão de riscos em segurança da informação;
- **ISO/IEC 22301** – Continuidade de negócios e recuperação de desastres.

---

1. Política de Acesso e Controle de Usuários

Objetivo: Garantir que apenas usuários autorizados tenham acesso a dados e sistemas específicos, de acordo com sua função e necessidade dentro da organização.

Justificativa: O controle de acesso é essencial para minimizar o risco de vazamentos de dados, acessos indevidos e falhas humanas. Ao limitar o acesso com base em perfis de função, garante-se que os usuários não tenham mais permissões do que o necessário para realizar suas tarefas.

Ações:

- Implantar controle de acesso baseado em perfil de função (RBAC).
- Realizar autenticação com múltiplos fatores (2FA) para sistemas críticos.
- Adotar a política de menor privilégio.
- Realizar revisões semestrais de acessos e permissões.
- Registrar e auditar todos os acessos a sistemas sensíveis.

Base na ISO/IEC 27002: Seções sobre controle de acesso.

---

2. Política de Uso de Dispositivos Móveis e Redes

Objetivo: Proteger a infraestrutura da empresa contra acessos inseguros por meio de dispositivos móveis e redes externas ou não confiáveis.

Justificativa: Dispositivos móveis e conexões externas (como Wi-Fi público) representam vetores comuns de ataque. Sem uma política clara, aumentam os riscos de vazamentos de dados, malwares e acesso indevido.

Ações:

- Adotar solução de MDM (Mobile Device Management) para monitorar e controlar dispositivos móveis corporativos.
- Proibir o uso de redes públicas para acessar sistemas da empresa, salvo com VPN corporativa.
- Bloquear conexões de dispositivos móveis não autorizados à rede interna.
- Restringir o uso de mídias removíveis (pendrives, HDs externos).
- Realizar treinamentos regulares sobre o uso seguro de dispositivos móveis.

Base na ISO/IEC 27002: Seções sobre segurança em dispositivos móveis e conectividade.

---

3. Diretrizes para Resposta a Incidentes de Segurança

Objetivo: Garantir uma resposta rápida e eficaz diante de qualquer evento que comprometa a segurança da informação da empresa.

Justificativa: A resposta eficiente a incidentes é fundamental para mitigar danos, preservar evidências e restabelecer operações com agilidade. Empresas que possuem processos definidos reduzem significativamente os impactos de ataques cibernéticos.

Ações:

- Estabelecer um plano de resposta a incidentes, com papéis e responsabilidades claras.
- Implantar sistemas de monitoramento de logs e alertas.
- Utilizar IDS/IPS para detectar comportamentos anômalos.
- Treinar a equipe sobre como identificar e reportar incidentes.
- Criar canais internos para reporte seguro e ágil de incidentes.
- Realizar simulações periódicas de resposta a incidentes.

Base na ISO/IEC 27035: Diretrizes para gestão de incidentes de segurança da informação.

---

4. Política de Backup e Recuperação de Desastres

Objetivo: Garantir a continuidade dos serviços e a recuperação de dados em caso de falhas, perdas acidentais, ataques ou desastres.

Justificativa: A perda de dados pode comprometer a continuidade do negócio. Backups regulares e bem armazenados permitem a recuperação rápida e minimizam o tempo de indisponibilidade.

Ações:

- Realizar backups automáticos diários dos dados críticos.
- Armazenar cópias em locais físicos seguros e na nuvem.
- Verificar periodicamente a integridade dos backups.
- Testar procedimentos de recuperação regularmente (DRP).

- Manter documentado o Plano de Continuidade do Negócio (PCN).

Base na ISO/IEC 22301: Sistema de gestão para continuidade de negócios.

Essas políticas foram pensadas considerando as limitações técnicas e financeiras comuns a pequenas empresas, mas sem comprometer a segurança da informação, a conformidade legal (como a LGPD) e a confiança dos clientes e parceiros.