Desenvolvimento de Políticas de Segurança para uma pequena empresa

Conjunto de políticas de Segurança:

**Políticas de acesso:**

1. **Princípio do menor privilégio:** Cada usuário deve ter apenas o acesso necessário para realizar suas tarefas.

* **Justificativa:** reduz riscos, porque mesmo se a conta for comprometida, o impacto é limitado.

1. **Segregação de funções:** Divide responsabilidades (ex: quem aprova não pode também criá-los
   * **Justificativa:** evita fraudes internas e erros, garantindo dupla checagem.
2. **Autenticação forte:** exige senhas seguras, autenticação multifator (MFA), etc.
   * **Justificativa:** dificulta ataques de roubo de senha, aumentando a segurança.
3. **Revisão periódica de acessos:** checagem regular para remover acessos desnecessários.
   * **Justificativa:** remove acessos obsoletos, diminuindo vulnerabilidades de contas inativas.

**Políticas de controle:**

**1.DAC – Discretionary Access Control**

* + Como funciona: o administrador de um recurso (arquivo, pasta, banco de dados) decide quem pode acessar.
  + Justificativa: dá flexibilidade, pois o criador do recurso controla diretamente.

**2. Mac – Mandatory Access Control**

* + Como funciona: regras fixa e rígidas, definidas pela **organização** (não pelo usuário). Normalmente baseia-se em **rótulos de segurança.**
  + **Justificativa**: garante que informações sensíveis só sejam acessadas por quem tem a devida autorização, sem depender de decisões individuais.

**3. RBAC – Role-Based Access Control**

* + **C**omo funciona: o acesso é concedido de acordo com a **função/cargo (role)** do usuário.
  + **Justificativa:** simplifica a administração de permissões em grandes organizações, já que o acesso vem do cargo/função.

4. **ABAC – Attribute-Based Access Control**

* + **Como funciona:** o acesso depende de **atributos** do usuário, do recurso e do contexto.
  + **Justificativa:** permite regras mais dinâmicas e detalhadas, alinhadas ao contexto e à necessidade real do usuário.

**Políticas de Uso de Dispositivos Móveis**

1. **Autorização prévia para uso de dispositivos pessoais:**  
   O uso de celulares, tablets ou notebooks pessoais para fins corporativos deve ser previamente autorizado pela área de TI.  
   • **Justificativa:** garante controle sobre dispositivos conectados à rede e reduz riscos de segurança.
2. **Proteção de acesso ao dispositivo:**  
   Todos os dispositivos devem ter senha, PIN ou autenticação biométrica configurados.  
   • **Justificativa:** impede acessos não autorizados em caso de perda, roubo ou uso indevido.
3. **Instalação de aplicativos autorizados:**  
   É proibida a instalação de aplicativos não aprovados pela organização em dispositivos que acessam dados corporativos.  
   • **Justificativa:** evita malware, vazamento de dados e comprometimento da rede.
4. **Criptografia e proteção de dados:**  
   Dados corporativos armazenados em dispositivos móveis devem estar criptografados.  
   • **Justificativa:** protege informações sensíveis mesmo que o dispositivo seja comprometido.
5. **Comunicação de incidentes:**  
   Qualquer perda, roubo ou suspeita de violação deve ser comunicada imediatamente ao setor de TI.  
   • **Justificativa:** permite resposta rápida e mitigação de riscos de segurança.

**Políticas de Uso de Redes**

1. **Acesso controlado à rede corporativa:**  
   Apenas dispositivos e usuários autorizados podem se conectar à rede interna ou Wi-Fi corporativa.  
   • **Justificativa:** reduz o risco de intrusões e acessos não supervisionados.
2. **Proibição de compartilhamento de credenciais:**  
   É vedado o compartilhamento de senhas de rede, VPN ou sistemas internos.  
   • **Justificativa:** evita comprometimento de contas e rastreamento inadequado de atividades.
3. **Uso responsável da rede:**  
   O uso da internet corporativa deve ser restrito a fins profissionais. Downloads, streaming e acesso a sites não relacionados ao trabalho são proibidos.  
   • **Justificativa:** garante desempenho da rede e evita exposição a conteúdos maliciosos.
4. **Monitoramento e auditoria:**  
   O tráfego da rede pode ser monitorado pela área de TI para fins de segurança e conformidade.  
   • **Justificativa:** permite identificar comportamentos suspeitos e prevenir incidentes.
5. **Segurança em redes externas:**  
   O acesso a sistemas corporativos por redes públicas (Wi-Fi abertas) deve ser feito apenas via VPN segura.  
   • **Justificativa:** protege comunicações contra interceptação e vazamento de dados.

**Política de Backup e Recuperação de Desastres**

O objetivo principal desta política é garantir a disponibilidade e a integridade dos dados críticos da empresa, permitindo uma recuperação rápida e completa após qualquer falha (humana, técnica ou de segurança).

**1 - Princípios de Backup**

Para uma pequena empresa com recursos limitados, a política se baseia na prática essencial da Regra 3-2-1.

**1.1 Cópia Off-site** - Pelo menos uma cópia deve estar armazenada fora do local de trabalho (off-site) (ex: nuvem ou local remoto fisicamente seguro). Protege contra desastres físicos (incêndio, roubo, enchente) que possam destruir todos os ativos no local principal.

**1.2 Mídias Diferentes** - As cópias devem ser armazenadas em pelo menos dois tipos de mídias diferentes (ex: disco rígido local e nuvem, ou servidor local e HD externo). Protege contra falhas de hardware específicas (ex: falha na marca X de disco).

**1.3 Cópias** - Devem existir pelo menos três cópias dos dados (o original em produção e dois backups). Garante redundância. Se o sistema principal falhar, há duas alternativas para a recuperação.

**2 - Tipos e Frequência de Backup**

A política deve focar em dados críticos, como informações de clientes, dados financeiros e arquivos essenciais de operação.

**2.1 - Tipo de Dado/Sistema**

Dados Críticos (Banco de Dados, Servidor de Arquivos)

Estações de Trabalho (Desktops e Notebooks)

**2.2 - Frequência**

Diária, fora do horário comercial (Janela de Backup).

Semanal ou acionada por evento.

**2.3 - Tipo de Backup**

Diferencial (salva as alterações desde o último Full) para agilidade na execução.

Full (Completo) semanalmente.

**2.4 - Retenção**

Últimos 30 dias (diários) e 12 meses (mensais).

Últimas 4 versões (máximo de 30 dias).

Justificativa: A frequência diária é crucial para a maioria dos negócios, limitando a Perda Máxima de Dados Aceitável (RPO) ao trabalho de um dia. A combinação de Diferencial/Full otimiza o tempo de execução do backup e a velocidade de restauração.

**2.5 - Parâmetros Críticos de Recuperação (RTO e RPO)**

Essas métricas definem o objetivo do Plano de Recuperação de Desastres:

**RTO (Objetivo de Tempo de Recuperação)**: É o tempo máximo tolerável para que um sistema ou serviço volte a funcionar após uma interrupção.

**Proposta para pequenas e médias empresas**.: 4 a 8 horas para sistemas críticos (ex: e-commerce, sistema financeiro) e 24 horas para sistemas secundários.

**RPO (Objetivo de Ponto de Recuperação)**: É a quantidade máxima de dados que a empresa pode aceitar perder (tempo entre o último backup e o incidente).

**Proposta para pequenas e médias empresas**.: 24 horas (dado o backup diário).

Justificativa: Definir RTO e RPO é fundamental para dimensionar a solução de backup e garantir que a recuperação atenda às necessidades de continuidade do negócio.

**2.6 - Procedimentos de Recuperação de Desastres**

O PRD é a parte acionada para reverter uma situação de desastre.

**Ação Proposta:**

**Testes Regulares de Restauração**: Pelo menos trimestralmente, o Coordenador Técnico (ou terceirizado) deve realizar um teste simulado de restauração para validar se os backups estão íntegros e se o RTO é atingível.

**Procedimento de Declaração de Desastre**: O Gerente de Incidentes é o único autorizado a "declarar desastre" (ex: ataque de ransomware ou falha de servidor irrecuperável).

**Local de Recuperação**: Usar o local off-site (nuvem) como o principal ponto de restauração, garantindo que a infraestrutura esteja separada do ambiente de produção afetado.

**Recuperação em Plataforma Alternativa:** Em caso de perda total de hardware, a prioridade é restaurar o serviço principal (ex: ERP, e-mail) em máquinas virtuais ou serviços em nuvem temporários.

Justificativa: Os testes regulares são a prova de que o plano funciona. A recuperação em uma plataforma alternativa, seja temporária ou em nuvem, garante a continuidade dos serviços essenciais, minimizando a paralisação operacional e financeira.

**Diretrizes para Resposta a Incidentes de Segurança**

O Plano de Resposta a Incidentes, é essencial para garantir que a empresa reaja de forma rápida, organizada e eficaz a qualquer evento de segurança (como um ataque cibernético, vazamento de dados ou falha de sistema), minimizando danos e perdas.

Fase 1: Preparação

Ação Proposta:

Criação de um Check-list de Emergência: Documento simples e impresso (além do digital) contendo os contatos chave, os tipos de incidentes mais prováveis (ex: ransomware, perda de notebook) e os primeiros passos de contenção.

Treinamento Mínimo: Todos os colaboradores devem saber o que é um incidente, como reportar imediatamente, e a quem e o que não fazer (ex: não tentar resolver o problema por conta própria, não desligar o computador da tomada).

Justificativa: A preparação é a fase mais crítica em pequenas e médias empresas., onde o tempo de resposta é vital. Ter um checklist simplificado e colaboradores treinados para o reporte imediato reduz o tempo de detecção e contenção, minimizando a propagação do dano.

Fase 2: Identificação e Triagem

Ação Proposta:

Canais de Reporte Único: Definir um único canal (ex: e-mail de emergência seguranca@empresa.com ou um número de telefone específico) para que qualquer funcionário, cliente ou parceiro reporte uma suspeita.

Avaliação Rápida (Triagem): O Coordenador Técnico (ou o Gerente de Incidentes, se o técnico estiver indisponível) deve avaliar a natureza, o que aconteceu? A extensão, quantos sistemas/dados foram afetados? e a Criticidade (qual o impacto no negócio/dados pessoais?) do incidente.

Preservação de Evidências: A equipe técnica deve coletar logs e imagens de sistemas de forma padronizada antes de tentar a recuperação, para análises posteriores e exigências legais.

Justificativa: A triagem rápida permite priorizar a resposta. Preservar evidências é fundamental para a análise da causa-raiz, eradicando o problema de vez, e para atender a possíveis demandas judiciais ou regulatórias.

Fase 3: Contenção

Ação Proposta:

Isolamento Imediato: Desconectar os dispositivos, servidores ou segmentos de rede afetados da rede principal e da internet.

Mudança de Senhas: Forçar a alteração de senhas de todos os usuários ou sistemas que possam ter sido comprometidos.

Justificativa: A contenção imediata (isolamento) é o principal objetivo para impedir a propagação, ex: evitar que um ransomware se espalhe para o servidor de backup e limitar os danos financeiros e de reputação.

Fase 4: Erradicação e Recuperação

Ação Proposta:

Erradicação: Remover a ameaça (ex: desinstalar malwares, fechar vulnerabilidades).

Recuperação: Restaurar os sistemas afetados a partir dos backups confiáveis, verificando a integridade dos dados antes de retornar à operação normal.

Reforço: Aplicar patches e reforçar as medidas de segurança, ex: habilitar autenticação de múltiplos fatores.

Justificativa: Garantir que o ambiente esteja completamente limpo e que os dados sejam restaurados de uma fonte segura e testada, assegurando o retorno à operação com maior segurança.

Fase 5: Lições Aprendidas e Documentação

Ação Proposta:

Reunião Pós-Incidente: O Gerente de Incidentes deve liderar uma breve reunião para analisar "o que funcionou" e "o que pode ser melhorado".

Atualização do Plano: Se um incidente expôs uma falha no PRI, (Plano de Resposta a Incidentes), ou no Checklist de emergência, este deve ser atualizado.

Relatório Final: Documentar a linha do tempo, as ações tomadas, os custos e as lições aprendidas.

Justificativa: Promove a melhoria contínua da segurança da empresa e serve como prova de conformidade.