Políticas de segurança - Minimarket

Como consultor de segurança da informação para um minimercado, o foco deve ser em políticas simples, diretas e adequadas ao porte da empresa, priorizando a proteção de dados de clientes e do negócio, a seguir veja as políticas aplicadas para garantir a segurança do sistema do estabelecimento.

Acessos e controle de usuários:

Garantir que apenas usuários autorizados tenham acesso aos sistemas e informações do minimercado.

- **Contas:** Cada colaborador deve ter uma conta de usuário individual e intransferível para acessar sistemas (PDV, controle de estoque, etc.). Contas genéricas ou compartilhadas são estritamente proibidas. O acesso deve ser concedido apenas aos recursos e dados essenciais para a execução do trabalho do colaborador.
  Evita que um erro ou ação maliciosa seja atribuída a uma conta genérica.
  Permite **rastrear** quem fez o quê, garantindo responsabilidade e facilitando auditorias internas
- **Senhas:** As senhas devem ter no mínimo 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos. Recomenda-se a troca de senhas a cada 90 dias. As senhas são confidenciais e não devem ser escritas ou compartilhadas com ninguém, nem mesmo com colegas ou supervisores.
  Protege contra **acessos não autorizados** aos sistemas de vendas e estoque.
- **Casos de encerramento ou mudanças de função:** Em caso de desligamento ou mudança de função, o acesso do colaborador a todos os sistemas deve ser revogado ou modificado imediatamente pelo administrador do sistema.
  É a principal defesa contra ex-colaboradores que poderiam usar credenciais antigas para acessar e causar danos ou roubar dados após o desligamento.
- **Segurança do PDV e dispositivos com acesso ao sistema interno:** Todos os computadores com acesso aos sistemas devem ser configurados para bloquear a tela automaticamente após o fim do expediente ou longo período de inatividade, exigindo a senha do usuário para desbloqueio.
  Previne que clientes ou pessoas não autorizadas usem o PDV, o computador do escritório ou o sistema de estoque quando o colaborador se ausenta.

Uso de dispositivos moveis e redes:

Estabelecer regras para o uso de dispositivos móveis, sejam eles da empresa ou pessoais.

- **Uso de aparelho móvel da empresa:** Os dispositivos fornecidos pela empresa devem ser usados predominantemente para fins de trabalho. O uso pessoal deve ser minimizado. A instalação de aplicativos deve ser limitada a softwares relacionados ao trabalho e autorizados pela gestão. Aplicativos de fontes não oficiais são proibidos.
  Dispositivos corporativos são ferramentas de trabalho. Restringir apps evita a instalação de *malwares* e *spywares* que possam comprometer dados da loja.
- **Proteção de aparelho móvel:** Todos os dispositivos (corporativos e pessoais usados para o trabalho) devem ter senha, PIN, padrão ou biometria para bloqueio de tela. Manter um software de segurança instalado e atualizado nos dispositivos corporativos. O sistema operacional e os aplicativos devem ser mantidos atualizados para garantir a proteção contra vulnerabilidades conhecidas.
  É a **segurança básica contra roubo físico**. Se o celular for roubado, a senha impede o acesso imediato aos dados ou às contas da empresa.
- **Utilização de dispositivos pessoais (BYOD):** O acesso a sistemas críticos da empresa (como PDV ou servidor de estoque) através de dispositivos pessoais não é necessário. É proibido armazenar dados sensíveis da empresa (listas de clientes, informações financeiras) em dispositivos pessoais.
  Garante que dados sensíveis não se espalhem por equipamentos que a empresa não pode gerenciar ou garantir a segurança, protegendo as informações de clientes e fornecedores.
- **Redes:** Dispositivos móveis que acessam a rede interna da loja para utilização do sistema devem usar uma rede Wi-Fi dedicada e protegida por senha forte separada da rede de clientes. É proibido acessar dados sensíveis da empresa (como sistemas de gestão, e-mails com informações financeiras) utilizando redes Wi-Fi públicas, abertas ou não confiáveis. Ao acessar sistemas da empresa remotamente, deve ser usada, preferencialmente, uma conexão VPN (Rede Privada Virtual) ou um protocolo de conexão segura (HTTPS). O Bluetooth e a função de compartilhamento de internet devem ser desativados quando não estiverem em uso, para evitar acessos não autorizados.
  Redes públicas são ambientes de alto risco para interceptação de dados (phishing/sniffing). A rede corporativa separada protege o PDV e os sistemas vitais do risco trazido por dispositivos pessoais (BYOD) ou clientes.

Diretrizes para Respostas a Incidentes de Segurança:

Procedimentos básicos a serem seguidos em caso de suspeita ou confirmação de um incidente de segurança.

- **Identificação de incidente:** Qualquer colaborador que notar atividade suspeita (computador lento, pop-ups estranhos, falta de acesso a dados, erro no PDV, ou movimentação incomum em estoque) deve reportar imediatamente. O incidente deve ser comunicado verbalmente à gerência ou ao responsável pela TI/Sistemas.
  Garante que incidentes sejam tratados rapidamente, **evitando a propagação** do problema para outros sistemas ou computadores da loja.
- **Contenção:** Desconectar o equipamento afetado da rede (Wi-Fi ou cabo de rede), mas não o desligar. Se possível e seguro, realizar um backup dos dados críticos recentes do sistema afetado antes de qualquer intervenção. Trocar imediatamente as senhas de todos os usuários que possam ter sido comprometidos ou que acessam o sistema afetado.
  O ato de desconectar da rede é a principal medida para **impedir a perda massiva de dados** ou que o incidente se espalhe pela rede.
- **Análise e Erradicação:** Avaliar a extensão do dano, a causa raiz e quais dados foram potencialmente afetados (seus ou de clientes). Remover a ameaça (ex: remover o *malware*, restaurar dados de um backup limpo, corrigir a vulnerabilidade).
  Assegura uma abordagem estruturada para voltar à operação normal o mais rápido possível.
- **Recuperação:** Recolocar o sistema afetado em produção, monitorando de perto. Garantir que todos os sistemas e dados estejam funcionando corretamente e acessíveis apenas por usuários autorizados.
  Transforma um evento negativo em aprendizado. Permite **fortalecer as defesas e** evitar que o mesmo erro aconteça novamente.
- **Documentar e melhorar:** Registrar o incidente, as ações tomadas e o resultado. Revisar as políticas de segurança e os procedimentos para evitar a recorrência do mesmo tipo de incidente.

Política de Backup e Recuperação:

Assegurar a disponibilidade e a integridade dos dados críticos da empresa (vendas, estoque, informações fiscais e de clientes) em caso de falha de sistema, erro humano ou desastre

- **Identificação de danos críticos:** Os seguintes dados são considerados críticos e devem ser incluídos no plano de backup: Banco de dados do PDV/Sistema de Gestão (vendas, estoque), dados fiscais e cadastros de clientes.
  A perda desses dados pode inviabilizar o cálculo de lucros, reposição de estoque e obrigações fiscais.
- **Rotina e frequência de backup:** Deverá ser realizado um backup completo do banco de dados do Sistema ao final de cada dia útil, após o fechamento do caixa e semanalmente ser realizado um backup completo de todos os arquivos e sistemas operacionais críticos.
  Reduz a **perda máxima de dados** a um dia de trabalho. Se o sistema falhar no meio da manhã, o minimercado perde apenas algumas horas de vendas.
- **Local de armazenamento:** Manter pelo menos 3 cópias dos dados, em 2 tipos diferentes de mídia, com 1 cópia armazenada fora do local físico. *Exemplo:* Cópia 1 (Servidor Local), Cópia 2 (HD Externo criptografado), Cópia 3 (Serviço de Nuvem seguro). A cópia em nuvem (Cópia 3) deve ser mantida para recuperação em caso de incêndio, inundação ou roubo no local do minimercado.
  Garante que se o prédio sofrer um desastre (roubo, incêndio), o negócio ainda terá os dados essenciais para se reerguer rapidamente.
- **Retenção de Backups:** Os backups diários devem ser mantidos por 7 dias, e os backups semanais completos por pelo menos 30 dias.
  O pior cenário é ter um backup que não funciona quando se precisa dele. Testar regularmente valida o processo e o equipamento.
- **Recuperação:** Pelo menos a cada 6 meses, um teste de restauração deve ser realizado para garantir que o backup é íntegro e que os procedimentos de recuperação funcionam no tempo esperado. Em caso de falha total do Sistema, o minimercado deve ter um procedimento manual documentado (ex: caderneta de anotação/planilha simplificada em tablet separado) para registrar as vendas, garantindo a continuidade das operações até a restauração do sistema.
  Garante a continuidade mínima do negócio. Permite que o minimercado continue vendendo e gerando receita.

Todas as políticas devem ser apresentadas de forma clara aos colaboradores e revisadas periodicamente para se adequar às mudanças no negócio ou na tecnologia. É fundamental fornecer treinamento regular sobre estas políticas, pois o erro humano é uma das maiores causas de incidentes de segurança em pequenas empresas.

Desenvolvido por:

Victor Domingos Moreira - 825155879

Lucas Gonçalves da Silva- 825113362

Victor de Morais Nelson - 825243925