UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI
DEPARTAMENTO DE COMPUTAÇÃO (DECOM)

Trabalho Prático I

Este trabalho, da disciplina de Segurança e Auditoria de Sistemas de Informação do curso de Sistemas de Informação da UFVJM, visa a elaboração de uma Política de Segurança da Informação (PSI) para uma empresa fictícia.

Docente: Eduardo Pelli

Discentes:
Alisson Alessandro Nunes Ferreira
Jevezon Jose Fernandes
Robson Luis Figueiredo Junior
Wender de Assis dos Santos

Segurança e Auditoria de Sistemas de Informação
Diamantina

Política de Segurança da Informação da Gabi Confeitaria

➢ ***Sobre nós:***

Constituída em 2019, a Gabi confeitaria atua na produção de bolos e doces personalizados para festas e eventos.

➢ ***Tamanho da Empresa***

- **Porte:** Micro empresa
- **Número de funcionários:** 4, sendo eles, confeiteiro, atendente, limpeza e entregador.

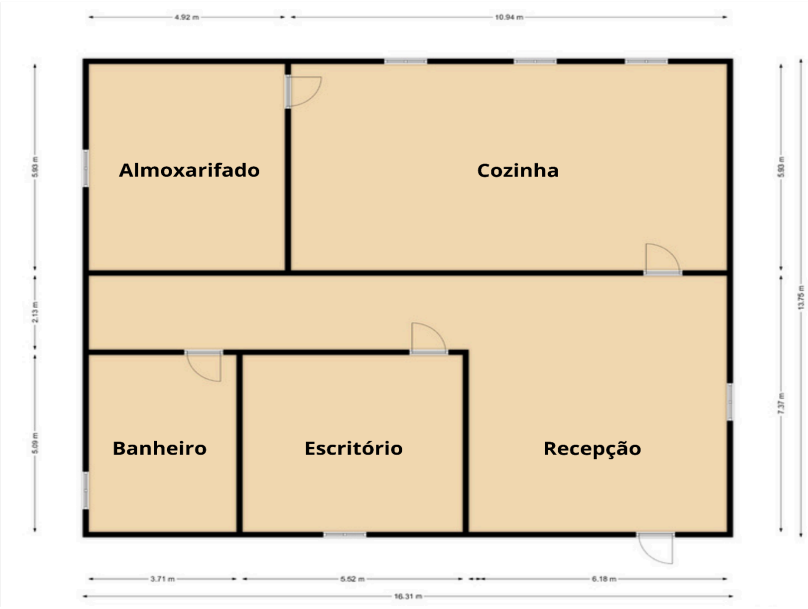
➢ ***Tipo de Negócio***

- **Setor:** Alimentício, especializado em confeitaria e produtos artesanais.

- **Produtos:** Bolos, tortas, doces gourmet, cupcakes, brownies, macarons, e outras sobremesas finas. Oferece também opções personalizadas para eventos, como casamentos, aniversários e confraternizações.

- **Serviços:** Venda direta ao consumidor na loja física, encomendas para eventos e delivery por aplicativos.

➢ ***Ambiente:*** Físico



➢ ***Missão***

A missão da Gabi Confeitaria é proporcionar experiências únicas e memoráveis através de produtos de alta qualidade, feitos artesanalmente, com ingredientes selecionados e atenção aos detalhes, promovendo momentos de felicidade e satisfação aos nossos clientes.

➢ **Valores**

- **Qualidade:** Compromisso com a excelência em todos os produtos, desde a seleção dos ingredientes até a apresentação final.
- **Criatividade:** Inovação constante nas receitas e no design dos produtos, sempre buscando surpreender os clientes.
- **Atendimento:** Atendimento personalizado e amigável, colocando o cliente no centro de todas as decisões.
- **Sustentabilidade:** Uso de práticas sustentáveis, reduzindo desperdícios e utilizando embalagens eco-friendly sempre que possível.
- **Tradição e Modernidade:** Respeito às receitas tradicionais, combinadas com técnicas modernas para criar produtos que agradem a todos os paladares.
- **Ética e Respeito:** Valorização de uma relação transparente e respeitosa com clientes, colaboradores e fornecedores, mantendo a integridade em todas as práticas do negócio.

➢ ***Vulnerabilidades***

Na Gabi confeitaria, tanto a estrutura física quanto a sistêmica estão sujeitas a vulnerabilidades, ameaças, riscos e impactos que podem comprometer suas operações.

➢ ***Estrutura Física***

- **Falta de manutenção:** Equipamentos como fornos, refrigeradores e máquinas de produção podem falhar se não forem mantidos regularmente.
- **Controle de acesso inadequado:** Portas e áreas de armazenamento podem não ser bem protegidas, permitindo acesso não autorizado.
- **Dependência de energia elétrica:** A confeitaria pode depender fortemente da eletricidade para a produção, conservação de produtos e uso de sistemas de caixa.

➢ *Estrutura Sistêmica*

- **Senhas fracas:** Uso de senhas fáceis de adivinhar ou senhas compartilhadas entre funcionários.
- **Sistemas desatualizados:** Falta de atualização de softwares, como sistemas de ponto de venda (PDV), expõe o negócio a vulnerabilidades conhecidas.
- **Backup inadequado:** Falta de backups regulares ou armazenamento inadequado dos mesmos.
- **Falta de firewall/antivírus:** Sistemas de segurança ausentes ou desatualizados deixam o ambiente digital vulnerável.

➢ *Principais Ameaças*

- **Estrutura Física**
- **Incêndios:** Devido ao uso de equipamentos de cozinha, há risco de incêndio em fornos, fogões ou fiação elétrica.
- **Roubo e vandalismo:** Risco de invasão ou furto, especialmente fora do horário de funcionamento.
- **Falta de energia:** Um apagão pode comprometer a produção e a conservação de ingredientes e produtos.
- **Inundações ou desastres naturais:** Vazamentos de água ou enchentes podem danificar o local físico e os equipamentos.

➢ **Estrutura Sistêmica**

- **Ataques cibernéticos:** Phishing, ransomware e malware podem comprometer dados financeiros, de clientes ou operações internas.
- **Fraude interna:** Colaboradores podem acessar indevidamente dados financeiros ou manipular o sistema de ponto de venda.
- **Quebra de equipamentos de TI:** Falha no sistema de caixa, na rede ou em dispositivos pode prejudicar as vendas e o atendimento ao cliente.

- **Interrupção de serviços de fornecedores de software:** Serviços de delivery ou pagamentos podem ser afetados se os sistemas parceiros tiverem falhas.

➔ Riscos

➢ Estrutura Física

Perda de produtos: Ingredientes perecíveis podem estragar durante interrupções prolongadas de energia, resultando em perdas financeiras.

Danos a equipamentos: Equipamentos caros como refrigeradores, fornos e batedeiras podem ser danificados por incêndios, mau uso ou desastres naturais.

Segurança do trabalho: Lesões de funcionários devido a práticas inadequadas de manuseio de equipamentos ou produtos quentes.

➢ Estrutura Sistêmica

- **Perda de dados financeiros:** Falta de backup pode levar à perda de dados de vendas e transações.
- **Roubo de dados pessoais:** Vazamento de dados de clientes, como informações de pagamento, pode levar a problemas legais e perda de reputação.
- **Interrupção nas vendas:** Uma falha no sistema de PDV pode impedir a finalização de compras, causando perda de receita.

➔ Impactos

➢ *Estrutura Física*

- Paralisação das operações: Incêndios, falhas elétricas ou inundações podem forçar o fechamento temporário da confeitaria, resultando em perda de receita.
- Custos de reposição: Reparos de equipamentos danificados ou substituição de ingredientes estragados geram despesas não planejadas.
- Comprometimento da qualidade: Falhas no armazenamento podem impactar a qualidade dos produtos, levando à insatisfação dos clientes.

➢ Estrutura Sistêmica

- Danos à reputação: Um ataque cibernético ou vazamento de dados pode abalar a confiança dos clientes.

- Multas e processos legais: Caso ocorra uma violação de dados, a confeitaria pode ser penalizada com multas por descumprimento de legislações como a LGPD.

- Queda nas vendas: A interrupção do sistema de venda online ou de delivery pode reduzir as vendas e o número de pedidos diários.

- Descontinuidade de negócios: Falta de backup ou ataques cibernéticos podem causar a perda de informações críticas, forçando a confeitaria a interromper operações até a recuperação.

Política de segurança

1. Introdução

Esta política de segurança visa proteger as informações e sistemas da Gabi Confeitaria contra ameaças, garantindo a integridade, confidencialidade e disponibilidade dos dados, especialmente em relação aos processos operacionais, dados de clientes e informações financeiras.

2. Objetivo

Proteger o ambiente digital e físico da confeitaria, minimizando riscos e garantindo a continuidade dos negócios. Esta política estabelece regras e diretrizes para o uso de sistemas de TI, proteção de dados e o comportamento seguro de todos os colaboradores.

3. Âmbito

Aplica-se a todos os colaboradores, prestadores de serviços, terceirizados e parceiros que têm acesso aos sistemas e informações da Gabi Confeitaria.

4. Princípios Gerais

- **Confidencialidade:** Garantir que as informações sensíveis da empresa, incluindo dados de clientes e transações financeiras, sejam acessíveis apenas por pessoas autorizadas.

- **Integridade:** Proteger os dados contra alterações indevidas, garantindo que as informações mantidas sejam corretas e completas.

- **Disponibilidade:** Assegurar que os sistemas e dados estejam disponíveis para uso sempre que necessário.

5. Diretrizes de Segurança

➢ *5.1 Controle de Acesso*

Apenas colaboradores autorizados têm acesso aos sistemas de informação.
O acesso a sistemas críticos, como o sistema de caixa e inventário, deve ser protegido por senhas fortes, com autenticação de dois fatores..
Senhas devem conter letras maiúsculas, minúsculas, números e caracteres especiais. Devem ser trocadas periodicamente, no máximo a cada 90 dias e não podem ser compartilhadas entre colaboradores.

➢ *5.2 Uso de Dispositivos*

Dispositivos que acessam a rede interna, computadores, tablets e celulares, devem estar protegidos por senhas e software de antivírus atualizado.
O uso de dispositivos pessoais para acessar sistemas corporativos deve ser previamente autorizado pela gerência.
Não é permitido o armazenamento de dados sensíveis, como informações financeiras em dispositivos pessoais sem criptografia adequada.

➢ *5.3 Backup e Recuperação de Dados*

Backups automáticos de sistemas financeiros e de inventário devem ser realizados diariamente.
Os backups devem ser armazenados em locais seguros e isolados da rede principal, de preferência em nuvem.
Devem existir procedimentos de recuperação de dados para casos de perda ou corrupção de informações.

➢ *5.4 Proteção de Dados de Clientes*

Dados de clientes, principalmente os sensíveis, devem ser armazenados em locais seguros, protegidos por criptografia.
Não é permitido compartilhar dados de clientes com terceiros, exceto quando estritamente necessário para a prestação de serviços ou cumprimento de obrigações legais.
Todos os dados de clientes devem ser eliminados de forma segura após o fim da sua utilidade, respeitando as leis de proteção de dados (LGPD).

➢ *5.5 Comunicação e E-mails*

Evitar o envio de informações sensíveis (como senhas ou dados de cartão de crédito) por e-mail sem proteção adequada, como o uso de criptografia.

E-mails recebidos devem ser verificados para evitar a instalação de malwares por meio de links ou anexos suspeitos.

➢ ***5.6 Monitoramento e Auditoria***

- Logs de acesso aos sistemas devem ser mantidos por um período mínimo de 6 meses para auditoria e monitoramento de incidentes de segurança.

- O monitoramento de acessos e atividades em sistemas críticos deve ser realizado para identificar tentativas de violação de segurança.

6. Responsabilidades

- **Gestores:** Responsáveis por garantir que seus subordinados cumpram a política de segurança e reportem qualquer incidente de segurança imediatamente.

- **Colaboradores:** Devem seguir as diretrizes estabelecidas nesta política, reportando comportamentos ou atividades suspeitas ao departamento responsável.

- **Equipe de TI/Segurança:** Responsável pela manutenção dos sistemas de segurança, backups e respostas a incidentes de segurança.

7. Resposta a Incidentes

- Todos os incidentes de segurança, como perda de dados, acessos não autorizados ou falhas nos sistemas, devem ser reportados imediatamente ao responsável pela segurança.

- A equipe de segurança deve avaliar o impacto do incidente e tomar as medidas necessárias para conter a ameaça, corrigir a vulnerabilidade e restaurar o sistema afetado.

8. Treinamento

Todos os colaboradores devem participar de treinamentos periódicos sobre boas práticas de segurança da informação e proteção de dados. Novos colaboradores devem ser treinados antes de iniciar o uso dos sistemas da confeitaria.

9. Atualização da Política

Esta política será revisada e atualizada periodicamente ou sempre que houver mudanças significativas no ambiente de tecnologia da confeitaria, visando mantê-la adequada e eficaz contra novas ameaças.

10. Consequências de Violação

O não cumprimento desta política poderá resultar em sanções disciplinares, incluindo advertências, suspensão ou demissão, dependendo da gravidade da violação. Casos graves poderão ser tratados conforme as leis vigentes.

Assinatura
Grupo C

Gabi Confeitaria
Data: 08/09/2024