

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Segurança da Informação

Gabriele Gonçalves de Azevedo

Gabriella de Oliveira Rodrigues

Gustavo Henrique Valeriano de Brito

Matheus Campos Madeira

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: Restaurante “O Gaulês”**

Orientador: Fábio Leandro Rodrigues Cordeiro

Belo Horizonte

2024

**SUMÁRIO**

[1. Introdução 4](#_Toc184324369)

[1.1. Objetivo 4](#_Toc184324370)

[1.2. Escopo 4](#_Toc184324371)

[2. Abrangência 5](#_Toc184324372)

[3. Princípios de Segurança 5](#_Toc184324373)

[3.1. Confidencialidade 5](#_Toc184324374)

[3.2. Integridade 5](#_Toc184324375)

[3.3. Disponibilidade 5](#_Toc184324376)

[4. Gerenciamento de Acesso 5](#_Toc184324377)

[4.1. Controle de Acesso 5](#_Toc184324378)

[4.2. Autenticação 5](#_Toc184324379)

[4.3. Autorização 6](#_Toc184324380)

[5. Segurança Física e Ambiental 6](#_Toc184324381)

[5.1. Proteção de instalações 6](#_Toc184324382)

[5.2. Controle de acesso físico 6](#_Toc184324383)

[5.3. Segurança ambiental 6](#_Toc184324384)

[6. Gestão de Incidentes de Segurança 6](#_Toc184324385)

[6.1. Resposta a incidentes 6](#_Toc184324386)

[6.2. Relatórios de incidentes 6](#_Toc184324387)

[7. Conscientização e Treinamento em Segurança 6](#_Toc184324388)

[7.1. Programa de conscientização 6](#_Toc184324389)

[7.2. Treinamento em segurança 7](#_Toc184324390)

[8. Avaliação e Melhoria Contínua 7](#_Toc184324391)

[8.1. Auditorias de segurança 7](#_Toc184324392)

[8.2. Revisão de políticas e procedimentos 7](#_Toc184324393)

[8.3. Análise de riscos 7](#_Toc184324394)

[8.4. Medição de desempenho 7](#_Toc184324395)

[9. Conformidade Legal e Regulatória 8](#_Toc184324396)

[9.1. Conformidade com leis e regulamentações 8](#_Toc184324397)

[9.2. Gerenciamento de vulnerabilidades e patches 8](#_Toc184324398)

[10. Responsabilidades 8](#_Toc184324399)

[10.1. Direção 8](#_Toc184324400)

[10.2. Equipe de segurança da informação 8](#_Toc184324401)

[10.3. Funcionários 8](#_Toc184324402)

[10.4 Descarte de informação 8](#_Toc184324403)

[11. Classificação da informação 8](#_Toc184324404)

[11.1 Criticidade 8](#_Toc184324405)

[11.2 Informações públicas 9](#_Toc184324406)

[11.3 Informações internas 9](#_Toc184324407)

[11.4 Informações Confidenciais 9](#_Toc184324408)

Uma política de segurança de modelo é um conjunto de diretrizes e práticas que visa proteger e gerenciar os recursos de uma organização, incluindo informações, ativos e tecnologias, e garantir a integridade, confidencialidade e disponibilidade desses recursos.

# 1. Introdução

## 1.1. Objetivo

Proteger as informações sensíveis do restaurante e de seus clientes, garantindo a confidencialidade, integridade e disponibilidade dos dados, minimizando riscos de vazamentos e incidentes de segurança, e promovendo uma cultura de conscientização e responsabilidade em relação à segurança da informação entre todos os colaboradores.

## 1.2. Escopo

**Dados Sensíveis:** Proteção de informações pessoais de clientes, como nomes, endereços, números de telefone e dados de pagamento.

**Informações Internas:** Segurança de dados financeiros, relatórios de vendas, receitas e informações de funcionários.

**Sistemas de TI:** Proteção de todos os sistemas de informação utilizados, incluindo software de gestão, plataformas de pedidos online e dispositivos móveis.

**Ambiente Físico:** Medidas de segurança para proteger o espaço físico onde os dados são armazenados, como escritórios e áreas de atendimento.

**Treinamento e Conscientização:** Inclusão de todos os colaboradores, garantindo que todos conheçam suas responsabilidades em relação à segurança da informação.

**Fornecedores e Terceiros:** Avaliação e controle de segurança das informações compartilhadas com fornecedores, parceiros de entrega e outras partes externas.

**Compliance:** Conformidade com legislações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) e normas de segurança alimentar (ISO 22000).

# 2. Abrangência

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os colaboradores, para todo o ambiente de trabalho, que venham a ter acesso e/ou utilizam as informações da empresa.

# 3. Princípios de Segurança

# 3.1. Confidencialidade

Assegurar que as informações do restaurante Gaulês sejam acessadas apenas por pessoas autorizadas, garantindo a privacidade dos dados de clientes e colaboradores.

## 3.2. Integridade

Garantir a consistência das informações e dos sistemas de informação do restaurante Gaulês, evitando alterações não autorizadas.

## 3.3. Disponibilidade

Proporcionar a disponibilidade do aplicativo e recursos de TI do restaurante Gaulês para que estejam sempre acessíveis quando necessários para garantir a continuidade do negócio.

# 4. Gerenciamento de Acesso

## 4.1. Controle de Acesso

O acesso a informações confidenciais deve ser restrito aos funcionários autorizados do restaurante Gaulês; O acesso físico a áreas críticas (como caixas registradoras e áreas administrativas) deve ser restrito.

## 4.2. Autenticação

Estabelecer processos de autenticação para verificar a identidade dos usuários que acessam os aplicativos de pedidos.

## 4.3. Autorização

Garantir que os usuários autorizados tenham permissões apropriadas para acessar recursos e sistemas dos aplicativos de pedido.

# 5. Segurança Física e Ambiental

## 5.1. Proteção de instalações

Implementar medidas para proteger as instalações físicas do restaurante Gaulês onde os sistemas de informação, documentos e recursos de TI estão localizados.

## 5.2. Controle de acesso físico

Estabelecer medidas de controle de acesso para impedir o acesso não autorizado às áreas críticas.

## 5.3. Segurança ambiental

Implementar medidas para proteger os recursos de TI físicos e documentos contra desastres naturais e outros riscos ambientais que impactem a continuidade do negócio.

# 6. Gestão de Incidentes de Segurança

## 6.1. Resposta a incidentes

Estabelecer um processo de resposta a incidentes para lidar com violações de segurança e minimizar seu impacto ao andamento do negócio. Isso inclui a identificação, contenção, erradicação e recuperação de incidentes de segurança.

## 6.2. Relatórios de incidentes

Os funcionários do restaurante Gaulês devem relatar todos os incidentes de segurança imediatamente à equipe de segurança da informação ou ao seu superior direto no setor.

# 7. Conscientização e Treinamento em Segurança

## 7.1. Programa de conscientização

Desenvolver e implementar um programa de conscientização sobre segurança para garantir que todos os funcionários compreendam suas responsabilidades e a importância da segurança da informação dentro do restaurante Gaulês.

## 7.2. Treinamento em segurança

Fornecer treinamento de brigadista, transporte e armazenamento das informações físicas e logicas da organização.

# 8. Avaliação e Melhoria Contínua

## 8.1. Auditorias de segurança

Realizar auditorias de segurança periodicamente no Restaurante Gaulês para avaliar a eficácia das políticas e práticas de segurança implementadas. Essas auditorias devem identificar áreas de melhoria e lacunas nos processos que possam afetar a segurança das informações dos clientes e a operação do restaurante.

## 8.2. Revisão de políticas e procedimentos

Revisar e atualizar regularmente as políticas e procedimentos de segurança do restaurante Gaulês, considerando as mudanças tecnológicas no setor de alimentação, ameaças emergentes (como novas formas de fraude de cartão de crédito) e as lições aprendidas com incidentes de segurança anteriores no ambiente de restaurantes.

## 8.3. Análise de riscos

Realizar análises periodicamente de risco específicas para identificar e avaliar os riscos de segurança associados às informações e ativos do Restaurante Gaulês. Isso inclui considerar riscos como o acesso não autorizado ao aplicativo de delivery, roubo de dados de clientes. Implementar medidas para mitigar esses riscos e proteger tanto os dados quanto a continuidade das operações do restaurante.

## 8.4. Medição de desempenho

Estabelecer métricas e indicadores-chave de desempenho (KPIs) para medir a eficácia dos programas de segurança e garantir que os objetivos de segurança sejam alcançados. Exemplos de KPIs podem incluir o número de incidentes de segurança registrados, o tempo de resposta a incidentes ou o nível de conformidade dos funcionários com os protocolos de segurança. Isso garante que os objetivos de segurança do restaurante sejam alcançados e mantidos.

# 9. Conformidade Legal e Regulatória

## 9.1. Conformidade com leis e regulamentações

Garantir que as políticas e práticas de segurança estejam em conformidade com as leis e regulamentações aplicáveis, incluindo leis de privacidade e proteção de dados; Dados pessoais dos clientes só devem ser usados para os fins para os quais foram coletados, como atendimento e marketing, sempre com consentimento.

## 9.2. Gerenciamento de vulnerabilidades e patches

Implementar um processo para identificar, avaliar e corrigir vulnerabilidades de segurança nos sistemas e aplicativos, incluindo a aplicação regular de patches de segurança.

# 10. Responsabilidades

## 10.1. Direção

A direção da organização é responsável por estabelecer e apoiar as políticas de segurança da informação e garantir que os recursos adequados sejam alocados para a gestão da segurança.

## 10.2. Equipe de segurança da informação

A equipe de segurança da informação é responsável pela implementação, monitoramento e manutenção das políticas e práticas de segurança e pela resposta a incidentes de segurança.

## 10.3. Funcionários

Todos os funcionários são responsáveis por seguir as políticas e práticas de segurança estabelecidas e por relatar qualquer incidente de segurança ou preocupações relacionadas à segurança da informação.

## 10.4 Descarte de informação

Todos os funcionários devem fazer o descarte correto das informações, sendo elas em papel trituradas e depois descartadas, visando reduzir possíveis vazamento de informações pelo descarte inapropriado.

# 11. Classificação da informação

## 11.1 Criticidade

As informações do restaurante devem ser classificadas de acordo com sua sensibilidade e criticidade.

## 11.2 Informações públicas

Podem ser divulgadas sem restrição (ex: cardápios, promoções).

## 11.3 Informações internas

Apenas acessíveis por funcionários autorizados (ex: controles de estoque).

## 11.4 Informações Confidenciais

Devem ser protegidas rigorosamente (ex: dados de clientes, transações financeiras).

Esta política de segurança de modelo abrange todos os aspectos importantes para garantir a integridade, confidencialidade e disponibilidade dos recursos e informações da organização.