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

**INSTRUÇÃO NORMATIVA DE SEGURANÇA DA INFORMAÇÃO: normas gerais do Restaurante “O Gaulês”**

Orientador: Fábio Leandro Rodrigues Cordeiro

Belo Horizonte

2024

**SUMÁRIO**

[OBJETIVO 1](#_Toc1304470283)

[ABRANGÊNCIA 1](#_Toc337463)

[DEFINIÇÕES 1](#_Toc1269277428)

[1.1 Para efeito desta norma 1](#_Toc888627048)

[1.1.1. Recursos de TIC do restaurante 1](#_Toc1435847312)

[1.1.2. Recursos de TIC particulares 1](#_Toc474190381)

[1.1.3. Redes sem fio (Wi-fi): 1](#_Toc1021058953)

[4. GESTÃO DE ACESSOS E PROTEÇÕES DE DADOS NO SISTEMA DE VENDAS 1](#_Toc2086670495)

[2.1 Acesso às informações: 1](#_Toc258261165)

[2.2 Autorização 1](#_Toc1874662643)

[2.3 Proteção de dados dos clientes 1](#_Toc1682676135)

[2.4 Backup 1](#_Toc27052616)

[2.5 Atualizações e manutenção 1](#_Toc680520502)

[2.6 Monitoramento e auditoria 1](#_Toc1313636719)

[3. RESPONSABILIDADES 1](#_Toc335322415)

[4. VENDAS Online 1](#_Toc370162051)

[4.1.1 Organização no espaço 1](#_Toc716103753)

[4.1.2 Pagamento 1](#_Toc1836284978)

[4.2.3 Atendimento ao cliente 1](#_Toc1401401630)

[4.2.4 Padrão de atendimento 1](#_Toc1851814780)

[4.3.1 Segurança da informação 1](#_Toc1423986878)

[4.3.2 Sistemas de vendas 1](#_Toc1414992220)

[4.4 Incidentes de segurança 1](#_Toc1936425613)

[4.4.1 Notificação de incidentes 1](#_Toc854605306)

[4.4.2 Resposta a incidentes 1](#_Toc1573833224)

[4.5 Manutenção e backup de sistemas 1](#_Toc1413372993)

[4.5.1 Backups 1](#_Toc714298725)

[4.5.2 Testes de recuperação 1](#_Toc186015122)

[5. Normas de Vendas Físicas para Restaurante 1](#_Toc472234172)

[5.1 Gestão de Acesso e Controle de Identidade 1](#_Toc1859086809)

[5.1.2 Controle de Acesso 1](#_Toc1313174183)

[5.1.3 Identificação e Autenticação 1](#_Toc878882028)

[5.1.4 Controle de Acesso Físico 1](#_Toc980159578)

[5.2. Segurança no Processamento de Pagamentos 1](#_Toc831092222)

[5.2.1 Segurança no Pagamento Eletrônico 1](#_Toc926369543)

[5.2.2 Pagamentos em Dinheiro 1](#_Toc688975048)

[5.2.3 Armazenamento Seguro de Comprovantes 1](#_Toc1460962432)

[5.2.4 Análise de Transações 1](#_Toc1650456999)

[5.3. Proteção de Dados e Privacidade 1](#_Toc1621517661)

[5.3.1 Coleta e Tratamento de Dados 1](#_Toc1212424833)

[5.3.2 Retenção e Exclusão de Dados 1](#_Toc1215186694)

[5.3.3 Conscientização sobre LGPD 1](#_Toc201803949)

[5.4. Monitoramento, Auditorias e Relatórios 1](#_Toc648276211)

[5.4.1 Implementação de Ferramentas de Monitoramento 1](#_Toc1556573346)

[5.4.2 Auditorias Periódicas 1](#_Toc1304189544)

[5.4.3 Relatórios Gerenciais 1](#_Toc818971023)

[5.5. Gestão de Incidentes e Resposta a Falhas 1](#_Toc775497140)

[5.5.1 Plano de Resposta a Incidentes 1](#_Toc2026717996)

[5.5.2 Procedimentos de Contingência 1](#_Toc824382311)

[5.5.3 Comunicação Interna e Externa 1](#_Toc1636031726)

[5.6. Treinamento Contínuo 1](#_Toc647658373)

[5.6.1 Capacitação em Segurança da Informação 1](#_Toc878766170)

[5.6.2 Simulações de Cenários 1](#_Toc769562817)

[5.7. Conformidade Legal e Regulatória 1](#_Toc864242905)

[5.7.1 Revisão Periódica da Legislação 1](#_Toc1341402687)

[5.7.2 Relatórios de Conformidade 1](#_Toc772327613)

[5.8. Segurança Física do Ambiente 1](#_Toc573011044)

[5.8.1 Controle de Acesso 1](#_Toc2101447027)

[5.8.2 Monitoramento Contínuo 1](#_Toc1366219304)

[6. Norma Inovadora: Programa de Monitoramento por Análise Comportamental com Inteligência Artificial (IA) no Ponto de Venda 1](#_Toc285681921)

[6.1. Descrição da Norma 1](#_Toc1124355565)

[6.2. Componentes da Norma 1](#_Toc1956941838)

[6.2.1. Implementação da Análise Comportamental por IA 1](#_Toc759907623)

[6.3. Prevenção Proativa de Fraudes 1](#_Toc254917438)

[6.4. Proteção Ética e Privacidade 1](#_Toc621719819)

[6.5. Estrutura de Resposta Integrada 1](#_Toc377746118)

[6.6. Feedback para Melhoria Contínua 1](#_Toc813768650)

[6.7. Benefícios Esperados 1](#_Toc776175320)

[7. APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES 1](#_Toc89856949)

# OBJETIVO

Estabelecer regras e orientações para uso de recursos de tecnologia de informação, denominados de TIC, para o armazenamento e processamento de informações do restaurante o Gaulês. Proporcionando meios mais eficientes na troca de informações entre os parceiros e colaboradores, protegendo a vida humana e a saúde, promovendo mecanismos eficazes para aferir qualidade de produtos.

# ABRANGÊNCIA

É um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os colaboradores, fornecedores e sistemas envolvidos no processo de vendas, incluindo atendimento presencial e plataformas digitais.

# DEFINIÇÕES

## 1.1 Para efeito desta norma

## 1.1.1. Recursos de TIC do restaurante

São disponibilizados pelo restaurante e mantidos e destinados às atividades técnicas e/ou administrativas, para uso nos atendimentos dentro do Gaulês.

## 1.1.2. Recursos de TIC particulares

são dispositivos móveis de propriedade dos colaboradores.

## 1.1.3. Redes sem fio (Wi-fi):

Conjunto de recursos de provimento de conexão para colaboradores e clientes, deve estar exposto por todo o restaurante avisos com o nome e senha da rede wi-fi, com o objetivo de conscientizar que se deve conectar somente a esta rede, com senha. Administrada e mantida pelo Gaulês.

# 4. GESTÃO DE ACESSOS E PROTEÇÕES DE DADOS NO SISTEMA DE VENDAS

## 2.1 Acesso às informações:

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

## 2.2 Autorização

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

## 2.3 Proteção de dados dos clientes

Dados de pagamento devem ser processados por sistemas certificados que atendam às normas PCI-DSS, não é permitido o armazenamento de informações completas de cartões de crédito no sistema de vendas, dados pessoas só devem ser acessados para finalidades especificas e autorizadas.

## 2.4 Backup

Realizar backups diários das informações de vendas, armazená-los em local seguro.

## 2.5 Atualizações e manutenção

Manter todos os sistemas de vendas atualizados com os patches de segurança mais recentes, realizar verificações trimestral para identificar vulnerabilidades.

## 2.6 Monitoramento e auditoria

Monitorar continuamente os acessos ao sistema de vendas para identificar atividades suspeitas, registrar logs de acesso e transações por um período mínimo de três meses, realizar auditorias anuais nos sistemas para garantir conformidade com esta norma.

# 3. RESPONSABILIDADES

A equipe de T.I deve implementar e manter as medidas técnicas descritas nesta norma, os gestores devem garantir que os colaboradores sigam as diretrizes, colaboradores devem cumprir as regras descrita nesta norma para que tudo ocorra nos padrões e evite perda de dados, erros nos processos de atendimento e uso seguro das informações.

# 4. VENDAS Online

### 4.1.1 Organização no espaço

Os colaboradores devem garantir que os produtos estejam colocados de forma organizada e atrativa para o cliente, promoções vigentes do dia e/ou da semana devem ser devidamente informadas por meio de comunicação com o cliente ou em devidamente a mostra no restaurante.

### 4.1.2 Pagamento

O sistema de pagamento deve ser utilizado plataformas seguras de cobrança.

### 4.3.1 Segurança da informação

As informações sensíveis, como relatórios de vendas e dados financeiros, devem ser armazenadas em local seguro, que somente pessoas da gerência e proprietários tenham acesso. Os dados sensíveis caso forem armazenados em dispositivos do restaurante, devem ser criptografados.

As informações de vendas devem ser armazenadas apenas pelo tempo necessário, conforme a LGDP define.

### 4.3.2 Sistemas de vendas

O sistema de vendas da empresa deve ser protegido, por autenticação forte, somente deve ser acessado somente pelos colaboradores.

O sistema deve ser atualizado constantemente para mitigar vulnerabilidades.

Os dispositivos moveis que forem utilizados no restaurante devem ser de propriedade dele, sempre protegido por antivírus e firewall ativo.

## 4.4 Incidentes de segurança

### 4.4.1 Notificação de incidentes

Qualquer suspeita de violação de segurança ou incidente deve ser reportado imediatamente ao responsável pela segurança da informação.

### 4.4.2 Resposta a incidentes

Em caso de incidente, deve ser usado o plano de reposta a incidentes do restaurante para mitigar os possíveis danos.

## 4.5 Manutenção e backup de sistemas

### 4.5.1 Backups

Deve ser implementado um sistema de backup automático e regulares dos dados de vendas em locais seguros.

### 4.5.2 Testes de recuperação

Deve ser realizado testes de periodicamente para garantir a integridade e a capacidade de recuperação dos backups.

# 5. Normas de Vendas Físicas para Restaurante

## 5.1 Gestão de Acesso e Controle de Identidade

Garantir que apenas indivíduos autorizados tenham acesso aos recursos críticos do sistema de vendas e a dados sensíveis relacionados.

### 5.1.2 Controle de Acesso

Todos os funcionários devem possuir credenciais individuais e seguras para acesso ao sistema de vendas.

Implantar políticas de acesso com base no Princípio do Menor Privilégio (Least Privilege): cada colaborador deve ter acesso apenas às informações e funcionalidades necessárias para desempenhar suas funções.

### 5.1.3 Identificação e Autenticação

Exigir autenticação forte com senhas seguras ou métodos biométricos para acesso a sistemas de pagamento e dados sensíveis.

Implementar procedimentos para trocas periódicas de senhas.

### 5.1.4 Controle de Acesso Físico

Restringir o acesso físico às áreas críticas do restaurante, como estoque, servidores, e local onde os dados de clientes ou pagamentos são armazenados.

Monitorar a entrada de funcionários por meio de sistemas de controle físico, como leitores biométricos ou cartões de acesso.

## 5.2. Segurança no Processamento de Pagamentos

Objetivo: Proteger as informações financeiras e transacionais durante todo o processo de pagamento físico.

### 5.2.1 Segurança no Pagamento Eletrônico

Garantir que terminais de pagamento sejam regularmente atualizados e compatíveis com padrões de segurança da PCI-DSS (Payment Card Industry Data Security Standard). Validar que todas as transações sejam criptografadas no envio de dados e ao armazenar informações no sistema.

### 5.2.2 Pagamentos em Dinheiro

Implementar contagem diária de dinheiro com procedimentos claros de conferência.

Armazenar valores em cofres seguros e monitorar a movimentação com sistemas de câmeras.

### 5.2.3 Armazenamento Seguro de Comprovantes

Arquivar comprovantes físicos em local seguro e com acesso restrito.

Digitalizar documentos relevantes apenas se devidamente criptografados e protegidos.

### 5.2.4 Análise de Transações

Monitorar diariamente as transações de pagamento para identificar comportamentos ou padrões atípicos.

Utilizar sistemas de controle e alertas automáticos para detectar tentativas de fraudes ou falhas no sistema.

## 5.3. Proteção de Dados e Privacidade

Objetivo: Assegurar a proteção dos dados pessoais e financeiros dos clientes e funcionários, em conformidade com a legislação vigente (LGPD, GDPR, entre outras).

## 5.3.1 Coleta e Tratamento de Dados

Coletar apenas as informações essenciais para a conclusão da transação (nome, CPF, e dados financeiros necessários).

Informar aos clientes, de forma clara, sobre o uso, armazenamento e tratamento desses dados.

### 5.3.2 Retenção e Exclusão de Dados

Implementar políticas claras para retenção mínima de dados, apenas pelo período necessário.

Estabelecer procedimentos seguros para exclusão de dados de clientes que não forem mais necessários ou cujo consentimento foi revogado.

### 5.3.3 Conscientização sobre LGPD

Capacitar todos os colaboradores no que diz respeito às obrigações legais impostas pela LGPD e boas práticas de proteção de dados.

## 5.4. Monitoramento, Auditorias e Relatórios

Objetivo: Assegurar que as transações e operações sejam constantemente monitoradas para identificar riscos e garantir a integridade do processo de vendas.

### 5.4.1 Implementação de Ferramentas de Monitoramento

Utilizar soluções tecnológicas para monitorar operações em tempo real, especialmente no sistema de transações.

Configurar alertas para comportamentos fora do padrão.

### 5.4.2 Auditorias Periódicas

Realizar auditorias internas e externas periodicamente para validar a conformidade com as políticas de segurança e normas legais.

Verificar a integridade dos dados e comparar com os registros financeiros e de transação.

### 5.4.3 Relatórios Gerenciais

Gerar relatórios periódicos com análises sobre padrões de vendas, transações financeiras e uso de dados.

Assegurar que esses relatórios sejam revisados por gestores responsáveis.

## 5.5. Gestão de Incidentes e Resposta a Falhas

Objetivo: Estabelecer procedimentos claros para identificar, responder e mitigar incidentes relacionados a falhas ou ameaças.

### 5.5.1 Plano de Resposta a Incidentes

Criar um plano documentado para resposta a incidentes de segurança, incluindo:

* Fraudes no ponto de venda.
* Acesso não autorizado a dados financeiros.
* Falhas no sistema de pagamentos.

### 5.5.2 Procedimentos de Contingência

Ter planos alternativos para falhas de tecnologia, como a perda de conexão ou indisponibilidade de sistemas.

### 5.5.3 Comunicação Interna e Externa

Definir processos claros de comunicação, incluindo o acionamento de equipe técnica e a comunicação com as partes afetadas.

## 5.6. Treinamento Contínuo

Objetivo: Capacitar todos os colaboradores no uso seguro de ferramentas e boas práticas de segurança no dia a dia.

### 5.6.1 Capacitação em Segurança da Informação

Treinar funcionários com frequência em temas como:

* Segurança nos processos de pagamento.
* Privacidade de dados.
* Boas práticas no uso de senhas e sistemas.

### 5.6.2 Simulações de Cenários

Realizar simulações de incidentes para preparar a equipe para situações críticas.

## 5.7. Conformidade Legal e Regulatória

Objetivo: Assegurar que todas as normas, práticas e políticas estejam alinhadas às regulamentações legais locais, nacionais e internacionais.

### 5.7.1 Revisão Periódica da Legislação

Manter a equipe legal envolvida na revisão periódica das normas legais relacionadas a dados, transações financeiras e operações no ponto de venda.

### 5.7.2 Relatórios de Conformidade

Apresentar relatórios periódicos que comprovem a conformidade com as exigências legais.

## 5.8. Segurança Física do Ambiente

Objetivo: Minimizar o risco de ameaças físicas, como furtos, roubos e invasões.

### 5.8.1 Controle de Acesso

1. Utilizar câmeras de segurança em todas as áreas estratégicas.
2. Restringir a movimentação em áreas críticas.

### 5.8.2 Monitoramento Contínuo

Implementar sistemas de alarme e monitoramento para proteger locais críticos, como o estoque e a área de pagamentos.

## 6. Norma Inovadora: Programa de Monitoramento por Análise Comportamental com Inteligência Artificial (IA) no Ponto de Venda

Objetivo

Implementar uma solução baseada em Análise Comportamental por IA para monitorar transações e comportamentos no ponto de venda, a fim de identificar padrões atípicos, prevenir fraudes financeiras, proteger dados sensíveis e melhorar a experiência do cliente.

### 6.1. Descrição da Norma

O restaurante adotará uma solução tecnológica integrada que utiliza Inteligência Artificial para analisar comportamentos de clientes e funcionários durante as transações financeiras no ponto de venda físico. Essa análise se dará com base em dados comportamentais capturados de maneira ética e legal, sempre alinhada à proteção da privacidade.

### 6.2. Componentes da Norma

### 6.2.1. Implementação da Análise Comportamental por IA

A IA será configurada para monitorar aspectos comportamentais, como:

* Frequência de aproximação dos funcionários ou clientes ao sistema de pagamento.
* Interações atípicas ou mudanças no padrão de pagamento.
* Tempo de conclusão de transações.
* Comportamentos suspeitos no uso de métodos de pagamento.

Isso será realizado por meio de:

* Sensores de movimento e proximidade.
* Câmeras (com uso restrito e criptografado).
* Análise de dados transacionais.

## 6.3. Prevenção Proativa de Fraudes

A IA identificará padrões suspeitos em tempo real e enviará alertas automáticos para a equipe responsável.

Exemplos de comportamentos identificados:

* Tentativas de múltiplas transações com dados de pagamento em um curto período.
* Ações que indicam tentativas de violação de segurança no ponto de venda.
* Uso de métodos de pagamento incompatíveis com o histórico do cliente.

## 6.4. Proteção Ética e Privacidade

Os dados pessoais e sensíveis capturados serão anonimizados e utilizados exclusivamente para fins de monitoramento e segurança.

A equipe responsável pela análise deve ser treinada para assegurar o uso ético da IA, sempre alinhando-se às legislações de proteção de dados (LGPD ).

## 6.5. Estrutura de Resposta Integrada

Caso a IA identifique um padrão suspeito, a equipe de segurança e operações será notificada em tempo real para intervir.

A resposta poderá incluir:

* Contato direto com o cliente/funcionário envolvido.
* Revisão do histórico transacional.
* Encaminhamento para auditoria interna.

## 6.6. Feedback para Melhoria Contínua

A solução de IA deve ter um sistema de aprendizado constante. Por meio do monitoramento das respostas e dos resultados após a análise de alertas, a IA ajustará seus algoritmos automaticamente para aprimorar suas previsões.

## 6.7. Benefícios Esperados

1. Detecção e mitigação de fraudes em tempo real, reduzindo perdas financeiras.
2. Maior proteção de dados e transações financeiras, aumentando a confiança dos clientes no ambiente físico do restaurante.
3. Melhoria da experiência do consumidor, já que os processos de monitoramento reduzem situações invasivas ou atrasos nas transações.
4. Capacitação da equipe com dados precisos, uma vez que relatórios gerados pela IA podem oferecer insights valiosos para treinamento e revisão de processos.

**Conclusão**

A implementação dessas normas permitirá a criação de um ambiente seguro para as operações de vendas físicas no restaurante, alinhando os processos de negócio às melhores práticas de segurança da informação. É fundamental que essas políticas sejam revisadas periodicamente e ajustadas conforme o cenário tecnológico e regulatório evoluem.

# 7. APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES

**Autenticação** - Processo de verificação de identidade, em que um usuário ou sistema comprova quem é, geralmente por meio de senhas, tokens ou biometria.

**Backup** - Cópia de segurança de dados ou sistemas, criada para evitar perda de informações em caso de falhas ou ataques.

**Caixas registradoras** - Equipamento utilizado no comércio para registrar transações de vendas e calcular valores, muitas vezes integrado a sistemas de gestão.

**Colaboradores** – Funcionários do estabelecimento.

**Criptografados** - Dados convertidos em um formato ilegível sem a chave ou senha de decriptação, para garantir segurança e privacidade.

**Firewall** - Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

**IA** – Inteligência Artificial

**Incidentes a segurança** - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação e levando à perda de um ou mais princípios básicos de confidencialidade, integridade e disponibilidade.

**LGPD** - Lei Geral de Proteção de Dados

**Logs** - Registros automáticos de atividades em sistemas, úteis para monitoramento, auditoria e análise de segurança.

**Normas PCI-DSS** - Conjunto de padrões de segurança para proteger dados de cartões de pagamento, exigidos por bandeiras de cartões como Visa e Mastercard.

**Patches** - Atualizações ou correções de software, usadas para resolver vulnerabilidades, erros ou adicionar funcionalidades.

**TIC** – Tecnologia da informação e comunicação.

**Wifi** - Tecnologia de conexão sem fio que permite dispositivos se conectarem à internet ou a redes locais sem necessidade de cabos.