**INSTRUÇÃO NORMATIVA DE SEGURANÇA DA INFORMAÇÃO**

**NORMAS GERAIS DO RESTAURANTE**

[1. OBJETIVO 2](#_Toc2035999171)

[2. ABRANGÊNCIA 2](#_Toc1783050101)

[3. DEFINIÇÕES 2](#_Toc823714503)

[3.1 Para efeito desta norma 3](#_Toc1024201759)

[3.1.1. Recursos de TIC do restaurante 3](#_Toc1004194729)

[3.1.2. Recursos de TIC particulares 3](#_Toc909796183)

[4. Gestão de acessos e proteções de dados no sistema de vendas 3](#_Toc850379443)

[4.1 Acesso às informações: 3](#_Toc755844397)

[4.2 Autorização 3](#_Toc616512475)

[4.3 Proteção de dados dos clientes 3](#_Toc1088789164)

[4.4 Backup 3](#_Toc1814702848)

[4.5 Atualizações e manutenção 3](#_Toc1922794861)

[4.6 Monitoramento e auditoria 4](#_Toc43900682)

[5. Responsabilidades 4](#_Toc1965338529)

[6. Vendas 4](#_Toc313393053)

[6.1 Atendimento no local 4](#_Toc62061161)

[7. Legislação Trabalhista e de Segurança no Trabalho 4](#_Toc1292127527)

[7.1 Normas Regulamentadoras (NRs) do Ministério do Trabalho e Emprego (MTE) 4](#_Toc1741449822)

[7.2. Lei 6.514/77 (Lei de Segurança e Medicina do Trabalho) 5](#_Toc1524464438)

[7.3. Consolidação das Leis do Trabalho (CLT) 5](#_Toc1601490547)

[8. Legislação de Saúde Pública e Vigilância Sanitária 5](#_Toc1060797465)

[8.1. Lei 8.080/90 (Lei Orgânica da Saúde) 6](#_Toc1003297134)

[8.2. ANVISA (Agência Nacional de Vigilância Sanitária) 6](#_Toc696792031)

[8.3. Vigilância Sanitária Local 7](#_Toc521110854)

[8.4. Boas Práticas de Fabricação (BPF) 7](#_Toc1975674589)

[9. Legislação Ambiental 7](#_Toc401744219)

[9.1. Lei de Resíduos Sólidos (Lei 12.305/2010) 7](#_Toc2020103439)

[9.2. Legislação Municipal sobre Poluição Sonora e Ar 7](#_Toc1623596267)

[10. Legislação de Proteção ao Consumidor 8](#_Toc1940691790)

[11. Outras Normas Aplicáveis 8](#_Toc65287527)

[11.1. Normas Técnicas da ABNT 8](#_Toc344323622)

[11.2. Código de Posturas Municipais 8](#_Toc348681148)

[12. Normas de Segurança Contra Incêndios e Emergências 9](#_Toc681694342)

[12.1. NR 23 – Proteção Contra Incêndios 9](#_Toc1540238161)

[12.2. Corpo de Bombeiros e Inspeções 9](#_Toc174427207)

[13. Legislação de Proteção ao Consumidor 9](#_Toc1865817576)

[14. Legislação Municipal e Normas Técnicas 10](#_Toc125499094)

[15. Leis de Segurança da Informação 10](#_Toc1449089726)

[15.1. Lei Geral de Proteção de Dados (LGPD) - Brasil (Lei 13.709/2018) 10](#_Toc656142988)

[16. Normas Técnicas e Padrões de Segurança da Informação 11](#_Toc42430153)

[16.1. ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação (SGSI) 11](#_Toc936550666)

[16.2. ISO/IEC 27002:2013 - Código de Práticas para Controles de Segurança da Informação 12](#_Toc1866199945)

[16.3. NIST Cybersecurity Framework (CSF) 12](#_Toc1708813599)

[15.4. PCI DSS (Payment Card Industry Data Security Standard) 12](#_Toc393372889)

[17. Outras Legislações e Considerações 13](#_Toc653313662)

[17.1. Lei de Cibercrimes (Lei 12.737/2012 - Lei Carolina Dieckmann) 13](#_Toc1824007015)

# 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*

## *3.1 Para efeito desta norma*

## 3.1.1. 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.

## 3.1.2. Recursos de TIC particulares

são dispositivos móveis de propriedade dos colaboradores.

3.1.3. 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

## 4.1 Acesso às informações:

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 Autorização

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

## 4.3 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.

## 4.4 Backup

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

## 4.5 Atualizações e manutenção

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

## 4.6 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.

# 5. 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.

# 6. Vendas

## 6.1 Atendimento no local

O atendimento no local deve se manter um padrão por todos os colaboradores, tendo uma recepção ao entrar no restaurante, escolha da mesa para melhor atendimento, após escolha do cliente, conferir o pedido para evitar erros no preparo.

# 7. Legislação Trabalhista e de Segurança no Trabalho

## 7.1 Normas Regulamentadoras (NRs) do Ministério do Trabalho e Emprego (MTE)

As Normas Regulamentadoras (NRs) são obrigatórias no Brasil e visam regulamentar as condições de segurança e saúde no trabalho. Para restaurantes, algumas NRs que se aplicam diretamente incluem:

* **NR 6** – Equipamento de Proteção Individual (EPI): Define as obrigações dos empregadores e trabalhadores quanto ao fornecimento e uso de EPIs, como luvas, aventais, calçados de segurança e protetores auditivos, quando necessário.
* **NR 17** – Ergonomia: Regula as condições de trabalho relacionadas ao conforto e à saúde dos trabalhadores. Para restaurantes, isso pode incluir ajustes em áreas como a altura das bancadas, cadeiras adequadas, pisos antiderrapantes e posturas corretas para evitar lesões.
* **NR 18** – Condições e Meio Ambiente de Trabalho na Indústria da Construção: Embora essa norma seja mais voltada para a construção civil, em casos de reformas ou manutenção no restaurante, deve ser seguida para garantir a segurança durante esses períodos.
* **NR 23** – Proteção Contra Incêndios: Determina os requisitos para a instalação de sistemas de prevenção e combate a incêndios, como extintores e rotas de fuga adequadas. Também especifica a obrigatoriedade de treinamento para os funcionários.
* **NR 24** – Condições Sanitárias e de Conforto nos Locais de Trabalho: Essa norma trata das condições de higiene e conforto no ambiente de trabalho, incluindo banheiros adequados, iluminação e ventilação.

### 7.2. Lei 6.514/77 (Lei de Segurança e Medicina do Trabalho)

Essa lei estabelece a obrigatoriedade de ações preventivas para garantir a saúde e segurança dos trabalhadores, incluindo a criação de CIPA (Comissão Interna de Prevenção de Acidentes),

### 7.3. Consolidação das Leis do Trabalho (CLT)

A CLT contém uma série de normas relacionadas aos direitos trabalhistas que garantem condições adequadas de trabalho, como o intervalo para descanso, condições de saúde e segurança, e a proteção contra acidentes e doenças ocupacionais. Algumas de suas disposições relacionadas à segurança incluem:

* **Art. 157** – Obriga o empregador a adotar medidas de segurança para garantir a saúde e a integridade física dos trabalhadores.
* **Art. 166** – Estabelece que o empregador deve proporcionar condições adequadas para a execução de tarefas, prevenindo acidentes de trabalho.

# 8. Legislação de Saúde Pública e Vigilância Sanitária

A vigilância sanitária regula as condições de higiene e segurança alimentar para evitar doenças transmitidas por alimentos e garantir o bem-estar dos consumidores.

### 8.1. Lei 8.080/90 (Lei Orgânica da Saúde)

Regulamenta os sistemas de saúde no Brasil e estabelece as bases para a política de saúde pública. Embora não seja específica para restaurantes, ela influencia as normas de vigilância sanitária e as práticas de saúde pública que afetam os estabelecimentos de alimentos e bebidas.

## 8.2. ANVISA (Agência Nacional de Vigilância Sanitária)

A ANVISA define as normas de segurança alimentar e higiene em estabelecimentos que manipulam alimentos e bebidas. Algumas das principais regulamentações incluem:

* **Resolução RDC 216/2004:** Estabelece as condições mínimas exigidas para o funcionamento de serviços de alimentação, incluindo boas práticas de manipulação, armazenamento e controle de temperatura de alimentos, além de requisitos de higiene e instalações adequadas.

**Algumas das principais exigências incluem:**

* **Treinamento de Manipuladores:** Os funcionários que manipulam alimentos devem ser treinados em boas práticas de higiene.
* **Controle de Temperatura:** Os alimentos devem ser mantidos em temperaturas adequadas para evitar a proliferação de microrganismos nocivos.
* **Armazenamento Correto:** Alimentos perecíveis devem ser armazenados em condições adequadas, com separação de produtos crus e cozidos, por exemplo.
* **Resolução RDC 275/2002:** Regula as condições de funcionamento de estabelecimentos de alimentos em relação à higiene e controle de doenças transmissíveis por alimentos, como Salmonella, E. coli, entre outras. Ela exige que os restaurantes adotem práticas para evitar contaminações cruzadas e outras formas de contaminação alimentar.
* **Resolução RDC 306/2004:** Estabelece normas sobre a saúde e segurança dos manipuladores de alimentos, exigindo que os funcionários sejam treinados em práticas de higiene e prevenção de contaminação alimentar.

## 8.3. Vigilância Sanitária Local

As vigilâncias sanitárias estaduais e municipais podem ter regulamentações adicionais que devem ser seguidas, dependendo da localização do restaurante. Elas geralmente abordam aspectos como:

* Licenciamento sanitário do estabelecimento.
* Inspeções periódicas de higiene e segurança alimentar.
* Controle de pragas e limpeza do ambiente.

## 8.4. Boas Práticas de Fabricação (BPF)

A implementação de Boas Práticas de Fabricação é fundamental para garantir a segurança dos alimentos. Estas práticas são um conjunto de normas para garantir a produção, manuseio e armazenamento de alimentos de forma segura. Incluem:

* Higiene pessoal dos manipuladores de alimentos.
* Uso correto de utensílios e equipamentos.
* Controle rigoroso de temperatura para evitar a proliferação de microrganismos.

# 9. Legislação Ambiental

O restaurante deve também cumprir com as normas ambientais que regulam o descarte de resíduos e a utilização de recursos naturais.

## 9.1. Lei de Resíduos Sólidos (Lei 12.305/2010)

Estabelece as diretrizes para a gestão de resíduos sólidos no Brasil, o que inclui a obrigatoriedade de reciclagem e o manejo adequado dos resíduos gerados pelo restaurante, como embalagens, óleo de cozinha usado e restos de alimentos.

## 9.2. Legislação Municipal sobre Poluição Sonora e Ar

Muitas cidades possuem normas que regulam a poluição sonora e do ar. O restaurante deve respeitar as leis locais relacionadas ao limite de ruído (especialmente se houver música ao vivo ou outros ruídos) e controle de emissão de poluentes no ambiente.

# 10. Legislação de Proteção ao Consumidor

O Código de Defesa do Consumidor (Lei 8.078/1990) também se aplica aos restaurantes, pois garante que os direitos dos consumidores sejam respeitados, incluindo:

* **Garantia de segurança alimentar:** O restaurante é responsável pela qualidade e segurança dos produtos que serve, garantindo que não haja riscos à saúde do consumidor.
* **Informação sobre ingredientes e alergênicos:** O estabelecimento deve informar sobre os ingredientes presentes nos pratos e sobre potenciais alergênicos, de acordo com as regulamentações da ANVISA e outras autoridades sanitárias.
* **Atendimento e reclamações:** O restaurante deve ter um protocolo de atendimento para lidar com reclamações e garantir a satisfação do cliente.

# 11. Outras Normas Aplicáveis

## 11.1. Normas Técnicas da ABNT

A Associação Brasileira de Normas Técnicas (ABNT) oferece várias normas que podem ser aplicáveis a restaurantes, como:

* NBR 9077: Norma sobre segurança contra incêndio e pânico.
* NBR 14001: Sistema de gestão ambiental, que pode ser útil para restaurantes que desejam adotar práticas sustentáveis.
* NBR 15775: Normas de segurança alimentar.

## 11.2. Código de Posturas Municipais

Cada município tem seu próprio Código de Posturas, que regula diversos aspectos do funcionamento de estabelecimentos comerciais, como horários de funcionamento, limite de barulho, normas de construção, e outros aspectos relacionados à convivência urbana.

# 12. Normas de Segurança Contra Incêndios e Emergências

A segurança contra incêndios é uma das áreas mais críticas para restaurantes, dada a presença de equipamentos como fogões, fornos e fritadeiras, que podem representar risco de incêndio.

## 12.1. NR 23 – Proteção Contra Incêndios

A NR 23 exige que todos os estabelecimentos, incluindo restaurantes, tenham um plano de prevenção e combate a incêndios. A norma inclui:

* Extintores de incêndio: De acordo com o risco do local, deve-se ter extintores apropriados (por exemplo, CO2 ou pó químico) e bem distribuídos.
* Rotas de fuga**:** O restaurante deve ter rotas de fuga sinalizadas e acessíveis, permitindo a evacuação rápida e segura dos clientes e funcionários em caso de emergência.
* Treinamento de Funcionários**:** Os funcionários devem ser treinados periodicamente em como agir em situações de emergência, incluindo uso de extintores, evacuação e primeiros socorros.

## 12.2. Corpo de Bombeiros e Inspeções

Além da NR 23, os corpos de bombeiros estaduais e municipais também realizam inspeções periódicas para garantir que o restaurante cumpra todas as exigências de segurança contra incêndios e pânico. Eles verificam:

* O controle de materiais inflamáveis.
* O planejamento de segurança em caso de emergência.
* A presença de equipamentos adequados, como mangueiras, extintores, sinalizações de emergência, entre outros.

# 13. Legislação de Proteção ao Consumidor

O Código de Defesa do Consumidor (CDC) (Lei 8.078/1990) também se aplica aos restaurantes, principalmente em aspectos relacionados à segurança alimentar e ao bem-estar do cliente. O CDC garante que os consumidores tenham seus direitos respeitados, incluindo:

* Segurança dos Alimentos: O restaurante é responsável pela qualidade e segurança dos alimentos servidos. Se um cliente sofrer intoxicação alimentar devido a negligência do restaurante, o estabelecimento pode ser responsabilizado.
* Transparência e Informações sobre Produtos: O restaurante deve informar de forma clara os ingredientes dos pratos, especialmente alergênicos que possam causar reações adversas nos clientes.

# 14. Legislação Municipal e Normas Técnicas

Além das normas federais, a legislação municipal pode impor regras adicionais, principalmente em relação a licenciamento e inspeção sanitária. Por exemplo:

* Licenciamento sanitário: O restaurante deve obter a licença da vigilância sanitária local antes de iniciar suas operações.
* Posturas Municipais: Cada município tem seu Código de Posturas, que regula aspectos como o horário de funcionamento, a segurança pública nas redondezas e a limpeza das ruas.

# 15. Leis de Segurança da Informação

As leis de segurança da informação geralmente regulam a proteção de dados pessoais, o tratamento de informações sensíveis e a responsabilidade por incidentes de segurança. Essas leis podem ser de âmbito nacional ou internacional, e muitas delas se baseiam em regulamentações específicas para proteger a privacidade e a integridade dos dados.

## 15.1. Lei Geral de Proteção de Dados (LGPD) - Brasil (Lei 13.709/2018)

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde 2020, é uma das principais legislações de proteção de dados pessoais do país. Ela tem como objetivo garantir a privacidade e a segurança dos dados pessoais de indivíduos, definindo direitos e responsabilidades sobre o uso e o tratamento dessas informações.

**Principais aspectos da LGPD:**

* Consentimento: A coleta e o processamento de dados pessoais devem ser realizados com o consentimento explícito do titular dos dados, exceto em alguns casos específicos (ex.: cumprimento de obrigações legais).
* Finalidade: Dados devem ser coletados e utilizados para finalidades específicas e legítimas, e não podem ser utilizados para outras finalidades sem o consentimento do titular.
* Transparência: As empresas devem ser claras sobre como os dados são coletados, processados e compartilhados.
* Segurança: A LGPD exige que as empresas adotem medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, destruição, alteração e vazamentos.
* Notificação de incidentes: A LGPD obriga que as empresas notifiquem a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados em caso de incidentes de segurança que possam comprometer os dados pessoais.
* Penalidades: A LGPD prevê multas significativas, que podem chegar até 2% do faturamento anual da empresa, com limite de R$ 50 milhões por infração, e outras sanções, como a suspensão do tratamento de dados.

# 16. Normas Técnicas e Padrões de Segurança da Informação

Além das leis, existem várias normas e frameworks técnicos que fornecem orientações detalhadas sobre como proteger as informações e implementar boas práticas de segurança em uma organização. As mais relevantes incluem:

## 16.1. ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação (SGSI)

A ISO/IEC 27001 é uma norma internacionalmente reconhecida que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Ela ajuda as organizações a protegerem suas informações de maneira sistemática e eficiente, adotando uma abordagem baseada em riscos.

**Principais aspectos da ISO/IEC 27001:**

* Gestão de riscos: A norma exige que a organização realize uma avaliação de riscos para identificar e tratar riscos à segurança da informação.
* Controle de acesso: A norma orienta sobre a implementação de controles para garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis.
* Planos de resposta a incidentes: A ISO/IEC 27001 exige que a organização tenha um plano de resposta a incidentes de segurança, incluindo a identificação, monitoramento, análise e resposta a incidentes de segurança da informação.
* Auditoria e conformidade: A norma requer que a organização realize auditorias internas regulares para garantir que o SGSI esteja funcionando corretamente.

## 16.2. ISO/IEC 27002:2013 - Código de Práticas para Controles de Segurança da Informação

A ISO/IEC 27002 é uma norma complementar à ISO/IEC 27001, oferecendo um conjunto de práticas recomendadas para controles de segurança da informação. Ela aborda diversas áreas, como controle de acesso, segurança física, segurança de rede e continuidade de negócios.

## 16.3. NIST Cybersecurity Framework (CSF)

O NIST Cybersecurity Framework, criado pelo National Institute of Standards and Technology (NIST) dos Estados Unidos, é um conjunto de diretrizes para melhorar a cibersegurança das organizações. O framework é utilizado por muitas empresas, especialmente as de setores críticos, e abrange cinco funções principais:

* Identificar: Compreender os riscos de segurança da informação.
* Proteger: Implementar proteções para limitar o impacto de incidentes de segurança.
* Detectar: Monitorar sistemas para detectar possíveis incidentes de segurança.
* Responder: Desenvolver planos de resposta a incidentes e mitigar danos.
* Recuperar: Estabelecer estratégias para restaurar as operações após um incidente.

## 16.4. PCI DSS (Payment Card Industry Data Security Standard)

O PCI DSS é um conjunto de requisitos de segurança para qualquer organização que manipule informações de cartões de pagamento. O objetivo é garantir que os dados de pagamento dos clientes sejam protegidos contra acessos não autorizados, vazamentos e fraudes.

**Principais requisitos do PCI DSS:**

* Criptografia de dados: A norma exige que os dados de cartões de pagamento sejam criptografados quando armazenados ou transmitidos.
* Controle de acesso: Restrições de acesso baseadas em funções e necessidade de saber.
* Monitoramento e testes: As empresas devem monitorar suas redes e sistemas para detectar atividades suspeitas e realizar testes regulares de segurança.

# 17. Outras Legislações e Considerações

## 17.1. Lei de Cibercrimes (Lei 12.737/2012 - Lei Carolina Dieckmann)

No Brasil, a Lei Carolina Dieckmann (Lei 12.737/2012) define crimes relacionados à invasão de dispositivos eletrônicos e a violação de dados. A lei foi criada para punir atos como invasão de sistemas, vazamento de dados e fraudes eletrônicas.

As leis e normas de segurança da informação são fundamentais para garantir a proteção de dados e a segurança digital. As legislações, como a LGPD e a ISO/IEC 27001, oferecem frameworks que ajudam organizações a implementar práticas de segurança adequadas para proteger informações sensíveis, prevenir vazamentos de dados e atender às exigências legais. Além disso, com o aumento da criminalidade cibernética, o cumprimento dessas normas é fundamental para evitar penalidades e proteger a integridade das informações.