**INSTRUÇÃO NORMATIVA DE SEGURANÇA DA INFORMAÇÃO**

**Proteção de Dados Sensoriais e**

**Digitais dos Clientes**

[1. Objetivo: 3](#_Toc65834413)

[2. Definição de Dados Sensoriais 3](#_Toc1235507043)

[3. Coleta e Armazenamento de Dados Sensoriais 3](#_Toc2014436987)

[4. Uso de Tecnologias de Realidade Aumentada e Interatividade 3](#_Toc860694897)

[5. Proteção de Dados de Voz e Comandos Inteligentes 4](#_Toc301559332)

[6. Política de "Privacidade Sensorial" 4](#_Toc536848826)

[7. Controle e Acesso aos Dados Sensoriais 4](#_Toc1855947454)

[8. Auditoria e Monitoramento de Dados Sensoriais 5](#_Toc1865913005)

[9. Treinamento Contínuo de Funcionários 5](#_Toc1395929289)

[10. Conclusão: 5](#_Toc485445023)

## 1. Objetivo:

Esta norma tem como objetivo estabelecer diretrizes inovadoras para a proteção de dados sensoriais e digitais coletados no ambiente do restaurante, impactando diretamente o processo de vendas, a fim de proporcionar uma experiência segura, personalizada e tecnológica para os clientes, respeitando sua privacidade e a segurança das interações digitais.

## 2. Definição de Dados Sensoriais

Dados sensoriais referem-se às informações que são coletadas através de dispositivos tecnológicos ou interações que os clientes fazem durante sua experiência no restaurante. Exemplos incluem:

* Interações em telas táteis ou QR Codes: Preferências alimentares, seleções de pratos, escolhas de temperos ou bebidas, e avaliações durante ou após a refeição.
* Identificação biométrica (quando for implementada): A utilização da biometria facial ou impressões digitais para personalização de atendimento (ex: reconhecimento de cliente regular, sugestão de pratos baseados em históricos de consumo).
* Dados Ambientais: Informações extraídas do ambiente do restaurante, como a temperatura do local, tipo de música ou iluminação, que possam ser ajustadas com base nas preferências digitais dos clientes.

## 3. Coleta e Armazenamento de Dados Sensoriais

Os dados sensoriais devem ser coletados de maneira transparente, com a autorização expressa do cliente e uso para fins específicos relacionados à melhoria da experiência no restaurante.

* Consentimento Antecipado: O cliente deve ser informado sobre a coleta de dados sensoriais no momento da interação. Isso inclui, por exemplo, ao escanear um QR Code ou ao ativar funcionalidades de personalização (como reconhecimento facial ou de voz).
* Criptografia de Dados Sensoriais: Todos os dados sensoriais coletados durante a experiência no restaurante (seja via dispositivos ou sensores) devem ser criptografados em tempo real, tanto na transmissão quanto no armazenamento.
* Limitação no Armazenamento: Os dados sensoriais não devem ser armazenados por mais de 30 dias a partir da coleta, a menos que o cliente tenha autorizado explicitamente o armazenamento para personalização futura. O armazenamento deve ser feito em servidores isolados e seguros.

## 4. Uso de Tecnologias de Realidade Aumentada e Interatividade

Quando for implementado dispositivos de realidade aumentada (AR) ou outras formas de interatividade para enriquecer a experiência do cliente (ex: cardápios digitais interativos, visualização de pratos em 3D), a segurança da informação deve ser garantida.

* Proteção de Interações em AR: As interações realizadas em plataformas de AR devem ser protegidas para evitar captura de dados sensíveis (como preferências alimentares, escolhas específicas de pratos, ou interações de compra).
* Limitação de Coleta de Dados de Interação: Deve-se evitar a coleta excessiva de dados durante a experiência AR, restringindo-se àqueles essenciais para a melhoria do serviço e a personalização do pedido.

## 5. Proteção de Dados de Voz e Comandos Inteligentes

Com o aumento do uso de assistentes digitais (como Alexa, Google Assistant ou outros dispositivos IoT) no ambiente de restaurantes, como sistemas de pedidos via voz ou comandos automáticos para controle de ambiente, devem ser adotadas medidas para garantir a proteção das informações geradas por voz.

* Criptografia de Comandos de Voz: Todos os dados de voz, comandos ou interações devem ser criptografados de ponta a ponta, garantindo que informações sensíveis (como preferências alimentares ou pedidos) não sejam acessadas indevidamente.
* Descarte Automático: As gravações de voz devem ser descartadas após a execução do comando ou conclusão do pedido, a menos que o cliente tenha consentido previamente com o armazenamento para fins de personalização futura.

## 6. Política de "Privacidade Sensorial"

Criação de uma nova categoria de "privacidade sensorial" voltada para garantir que as informações coletadas através das interações físicas ou digitais do cliente não sejam usadas para invadir a privacidade dele.

* Controle do Cliente sobre seus Dados Sensoriais: O cliente pode optar por ativar ou desativar a coleta de dados sensoriais a qualquer momento, tanto para interações em dispositivos digitais quanto em interação direta com o ambiente do restaurante (ex: preferências de música, temperatura ou luz).
* Não Coleta de Dados Invasivos: O restaurante deve garantir que não sejam coletados dados sensoriais que possam ser considerados invasivos, como monitoramento de expressões faciais ou movimentos corporais sem a autorização do cliente. O foco deve ser sempre a melhoria da experiência e não o monitoramento.

## 7. Controle e Acesso aos Dados Sensoriais

Acesso aos dados sensoriais coletados deve ser restrito a funcionários autorizados e a tecnologias que garantam a confidencialidade e segurança.

* Acesso Restrito: Apenas gerentes de nível superior ou funcionários com funções específicas (ex: atendentes) devem ter acesso aos dados sensoriais, sempre com justificativa legítima (ex: personalização de pedido, ajustes no ambiente).
* Transparência com o Cliente: O cliente deve ser capaz de acessar, revisar ou até deletar os dados sensoriais armazenados sobre ele, seja via aplicativo, site ou diretamente no restaurante.

## 8. Auditoria e Monitoramento de Dados Sensoriais

A segurança de dados sensoriais deve ser auditada periodicamente para garantir conformidade com as diretrizes estabelecidas e detectar quaisquer vulnerabilidades:

* Auditorias Mensais: Realização de auditorias mensais para monitoramento do uso de dados sensoriais, revisão de acessos e garantias de conformidade com os princípios de privacidade.
* Análise de Riscos: A cada seis meses, deve ser feita uma análise de riscos para avaliar possíveis brechas de segurança nos sistemas que coletam, armazenam ou processam dados sensoriais.

## 9. Treinamento Contínuo de Funcionários

A equipe do restaurante deve passar por treinamento específico sobre como lidar com dados sensoriais, interações digitais e privacidade dos clientes.

* Treinamento de Segurança Digital e Sensoriais: Todos os funcionários, principalmente os que têm acesso direto aos sistemas de coleta e armazenamento de dados sensoriais, devem ser treinados sobre como proteger as informações e evitar o uso indevido.
* Atualizações Regulares: Treinamentos e workshops sobre novas tecnologias, regulamentações de segurança da informação e proteção de dados sensoriais devem ser realizados anualmente.

## 10. Conclusão:

A implementação desta norma visa criar um ambiente de restaurante mais seguro e respeitoso com a privacidade e dados sensoriais dos clientes, oferecendo uma experiência mais personalizada e segura, ao mesmo tempo em que adota tecnologias inovadoras para o setor. A proteção dos dados não se limita apenas a informações tradicionais, mas se estende também à interação digital e sensorial que caracteriza o futuro da experiência gastronômica.