| Nº: | ITR.POL.001 | Nome: | Política de cibersegurança pública |
|---|---|---|---|
| Versão: | 02 | Responsável: | Nicola Zágari |
| Classificação da Informação: | | | ( X ) Pública ( ) Interna ( )Confidencial |

# POLÍTICA DE CIBERSEGURANÇA PÚBLICA

## 1. OBJETIVO

Estabelecer as diretrizes e responsabilidades associadas à proteção de sistemas, programas, redes e pessoas no formato digital e em espaços cibernéticos.

## 2. ABRANGÊNCIA

Esta política aplica-se a todos os foodlovers que atuam na operação do iFood Pago, bem como a qualquer pessoa ou entidade que trabalhe para ou em nome do iFood Pago.

## 3. VIGÊNCIA

Este documento tem validade de dois anos a partir da data de sua publicação, podendo ser alterado a qualquer tempo e critério.

## 4. DEFINIÇÕES

**4.1.** Cibersegurança: Conjunto de ações que visam proteger sistemas, redes e equipamentos de invasões ou ataques cibernéticos.

**4.2.** Incidentes: Consideramos incidente de segurança da informação uma ocorrência que resulte em risco real ou potencial à confidencialidade, integridade ou disponibilidade de um sistema de informação

iFood Pago: Nome fantasia associado a negócios financeiros (MovilePay SCD).

## 5. DIRETRIZES

Atento às regulamentações do mercado o qual o grupo está inserido e alinhado aos objetivos estratégicos dos negócios, a política de segurança cibernética tem como diretrizes:

### 5.1. Pilares da segurança de informação

Com o objetivo de sustentar o comprometimento com a proteção dos ativos de nossa propriedade e/ou sob nossa guarda e responsabilidade, nos baseamos nos três pilares de segurança da informação:

- Garantir a confidencialidade para que as informações do iFood que formam a nossa receita de sucesso, sejam acessadas somente por pessoas autorizadas.
- Garantir que as informações do iFood estejam íntegras e seus sistemas sejam consistentes e confiáveis.

- Garantir a disponibilidade das informações.

### 5.2. Privacidade e proteção de dados pessoais

Respeitamos a sua privacidade e tratamos os seus dados pessoais como parte da nossa missão de proporcionar um serviço cada vez melhor. O iFood Pago possui o seu próprio Programa de Privacidade, incluindo, por exemplo, a Declaração de Privacidade para iFood Pago, que esclarece como o tratamento de dados pessoais dos clientes é realizado.

### 5.3. Classificação da informação

Para que as informações sejam acessadas apenas por pessoas autorizadas, estabelecemos diretrizes para classificação das informações de acordo com o seu grau de confidencialidade.

### 5.4. Conscientização

Para garantir a disseminação da cultura de segurança cibernética devem ser realizadas campanhas de conscientização, onde os colaboradores têm acesso a treinamentos, boas práticas e dicas de como aplicar segurança da informação em suas atividades diárias.

### 5.5. Gestão de riscos de segurança da informação

Para garantir a melhoria contínua da segurança da informação e da segurança cibernética, mantemos um processo de gestão de riscos estruturado com o objetivo de minimizar os impactos adversos nas operações e na integridade dos dados de iFoodPago.

### 5.6. Gestão de Incidentes de segurança da informação

Consideramos incidente de segurança da informação uma ocorrência que resulte em risco real ou potencial à confidencialidade, integridade ou disponibilidade de um sistema de informação ou das informações que o sistema processa, armazena e transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitável. O grupo conta com um time responsável pela resposta a incidentes durante todo seu ciclo de vida.

### 5.7. Gestão de vulnerabilidades

Manter um processo estruturado de gerenciamento de vulnerabilidades que considere a identificação de possíveis ameaças aos ativos de TI, bem como a implementação de patches, atualizações ou correções necessárias para mitigar as possibilidades de exploração de uma vulnerabilidade.

### 5.8. Gestão da continuidade do negócio

A nossa Gestão da Continuidade de Negócios estabelece um conjunto de estratégias para com medidas imediatas que devem ser tomadas frente a um cenário de crise, identificando os papeis e atribuindo responsabilidades a cada área envolvida.

## 6. PAPÉIS E RESPONSABILIDADES

### 6.1. Alta Direção

- Garantir a segurança das informações fornecidas à sociedade e ao mercado;
- Se comprometer com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

### 6.2. Segurança da Informação

- Desenvolver, implementar e revisar as políticas, procedimentos de Segurança da Informação que forneçam proteção adequada às informações e sistemas;
- Garantir a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

### 6.3. Gestores

- Assegurar que as práticas de Segurança da Informação definidas são observadas e seguidas por suas equipes, bem como difundir e manter a cultura de Segurança da Informação.

### 6.4 Foodlovers, prestadores de serviços e visitantes

- Conhecer e cumprir as determinações da política, norma e padrões de segurança da informação e segurança cibernética

## 7. DOCUMENTOS DE REFERÊNCIA

**7.1.** Resolução nº 4.893/2021.
**7.2.** Política de Cibersegurança interna.

## 8. HISTÓRICO

| Data | Versão | O que foi alterado? |
|---|---|---|
| **01/08/2023** | 1 | Primeira versão |
| **08/10/2024** | 2 | Alterações de texto nos capítulos:<br>Item 5.2<br>Item 5.5 |

| Versão | Elaborador (a) | Revisor (a) | Revisor (a) |
|---|---|---|---|
| 1 | Nome: Allana Brito | Nome: Felipe Thomé | Nome: Nicola Zágari |
| | Data: 01/08/2023 | Data: 22/09/2023 | Data: 05/03/2024 |

| | | | |
|---|---|---|---|
| Nº: | ITR.POL.001 | Nome: | Política de cibersegurança pública |
| Versão: | 02 | Responsável: | Nicola Zágari |
| Classificação da Informação: | | | ( X ) Pública ( ) Interna ( )Confidencial |

| | | | |
|---|---|---|---|
| 2 | Nome: Allana Brito | Nome: Rodrigo Sozza | Nome: Nicola Zágari |
| | Data: 08/10/2024 | Data 22/10/2024 | Data: 25/10/2024 |

| Versão | Aprovador (a) |
|---|---|
| 1 | Nicola Zagari |
| 2 | Diretoria Executiva em RD de 05/11/2024 |