POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1. OBJETIVO

A presente Política de Segurança da Informação e Cibernética ("**Política**") tem como objetivo estabelecer as diretrizes e responsabilidades relacionadas aos princípios e à gestão da confidencialidade, integridade e disponibilidade dos dados e sistemas de informação pertencentes ao iFood Pago no processo de gestão dos requisitos da Segurança da Informação e Cibernética, bem como garantir a capacidade da Instituição de prevenir, detectar e reduzir a vulnerabilidade a Incidentes de Segurança da Informação e Cibernética.

2. ABRANGÊNCIA

A presente Política abrange o iFood Pago e Foodlovers.

3. REFERÊNCIAS

- Legislação e Regulamentação do BACEN e CMN aplicáveis ao iFood Pago.
- ABNT NBR ISO 27001, norma padrão e a referência Internacional para a gestão da Segurança da informação.

4. DEFINIÇÕES

Adequação: significa garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo gestor da informação.

Autenticidade: significa a possibilidade de avaliação da propriedade como genuína, verificada e confiável (originais e não modificadas)l, assim como a confiança na validade de uma transmissão, mensagem ou do originador de uma mensagem (identidade de quem está enviando a informação).

BACEN ou **BCB:** refere-se ao Banco Central do Brasil.

CMN: refere-se ao Conselho Monetário Nacional.

Comitê de Riscos e Compliance ou **CRC:** refere-se ao Comitê de Riscos e Compliance do iFood Pago.

Foodlovers: colaboradores que atuam no iFood Pago.

iFood Pago ou **Conglomerado** ou **Instituição**:Refere-se ao Conglomerado Prudencial iFood Pago nº C0087346 (identificação BACEN) e as sociedades que dele fazem parte.

Incidente: fato ou evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, podendo comprometer a confidencialidade, integridade ou disponibilidade das informações, e até interromper um serviço ou processo, bem como qualquer situação que represente uma violação ou ameaça iminente de violação às políticas de segurança e demais normativos internos ou políticas de uso aceitável da Instituição.

PCI-DSS: refere-se à *Payment Card Industry Data Security Standard*.

RSFN ou **Rede do Sistema Financeiro Nacional:** significa a estrutura de comunicação de dados que tem por finalidade amparar o tráfego de informações no âmbito do Sistema Financeiro Nacional para serviços autorizados pelo BACEN.

SIEM: significa *Security Information and Event Management*, em português Gerenciamento de Informações e Eventos de Segurança.

SGSI: significa Sistema de Gestão da Segurança da Informação.

5. DIRETRIZES

5.1. Estrutura de Segurança de Informação e Cibernética

A estrutura organizacional de Segurança de Informação e Cibernética reflete a seleção de controles da gestão de segurança e é baseada no resultado da Avaliação de Riscos, nas orientações dos acionistas, no diagnóstico realizado e na legislação e regulamentação aplicável.

Essa estrutura garante que as responsabilidades sejam claramente definidas, implementadas e monitoradas em toda a organização, zelando pelo comprometimento de todos os níveis da Instituição com a segurança dos seus dados.

5.2. Diretrizes Gerais

A Segurança da Informação e Cibernética no iFood Pago observa, como diretrizes gerais, as estratégias internas, as normas NBR ISO IEC 27001 e 27002, bem como os padrões PCI-DSS, requerimentos BACEN e as boas práticas de mercado em segurança da informação e cibernética. As diretrizes gerais consideram modelo, natureza e complexidade dos negócios e das operações com o objetivo de implementar não apenas os controles tecnológicos, mas também os controles de processo, garantindo assim a governança na implementação do Sistema de Gestão da Segurança da Informação da organização.

Nesse sentido, são diretrizes gerais de Segurança da Informação e Cibernética:

(a) Proteger os dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;

(b) Zelar pela adequada classificação das informações e garantia da continuidade do processamento destas, conforme os critérios e princípios indicados nos normativos específicos;

(c) Zelar para que os sistemas e dados sob a responsabilidade do iFood Pago estejam devidamente protegidos e estejam sendo utilizados apenas para o cumprimento das nossas atribuições;

(d) Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados e tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados restritos e confidenciais;

(e) Realizar a manutenção e o gerenciamento de *softwares* antivírus, *firewall* e demais *softwares* de segurança instalados e atualizados, bem como a manutenção dos programas de computador instalados no ambiente;

(f) Prevenir, detectar e mitigar eventuais vulnerabilidades, que quando exploradas podem causar Incidentes relacionados com o ambiente cibernético; e

(g) Observar às leis e normas que regulamentam as atividades realizadas.

5.3. Pilares da Segurança da Informação e Cibernética

Para garantir a segurança das informações e Cibernética, os seguintes pilares são observados e considerados em toda tomada de decisão:

5.4. Ativos de Informação

Consideram-se ativos de informações todas as informações geradas ou desenvolvidas para o negócio que podem estar presentes de diversas formas, tais como: arquivos digitais, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, bancos de dados e conversas.

Independentemente da forma apresentada, compartilhada ou armazenada, os ativos de informação devem ser utilizados apenas para a finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

Todo ativo de informação de propriedade do iFood Pago deve ter um responsável devidamente classificado de acordo com os critérios estabelecidos e adequadamente protegido de quaisquer riscos ou ameaças que possam comprometer o negócio.

5.5. Implementação e Operação das Diretrizes de Segurança da Informação e Cibernética

Com base no Sistema de Gestão da Segurança da Informação e Cibernética, para implementação e operacionalização das diretrizes indicadas nesta Política, a Instituição deve:

(a) Formular um plano de tratamento de risco que identifica a ação apropriada a ser adotada pela direção, os recursos e as responsabilidades e prioridades para o gerenciamento dos riscos relacionados com a segurança da informação;

(b) Implementar plano para o tratamento de pontos de auditoria que estejam sob responsabilidade da área, atendendo aos objetivos de controle identificados;

(c) Implementar controles selecionados de acordo com o disposto nas regulamentações aplicáveis e boas práticas de segurança da informação;

(d) Definir como medir a eficácia dos controles ou grupos de controle selecionados e especificar como essas medidas são usadas, visando produzir resultados comparáveis e reproduzíveis;

(e) Definir o escopo, os limites da área e os processos envolvidos, em termos das características

do negócio, da organização, da localização, dos ativos e da tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo de controles;

(f) Implementar tecnologias e processos que identifiquem qualquer tentativa de violação de segurança da informação, bem-sucedidas ou não, além de eventos que possam causar Incidentes de segurança da informação;

(g) Realizar, a cada 6 (seis) meses, a análise crítica da eficácia dos controles, por meio do Comitê de Riscos e Compliance, para garantir que o escopo permanece adequado e que melhorias no processo de gestão de segurança são identificadas e implementadas;

(h) Gerenciar as operações de Segurança da Informação;

(i) Gerenciar os recursos de tecnologia sob sua custódia; e

(j) Implementar Políticas, Padrões e Procedimentos e outros controles que sejam capazes de permitir a pronta detecção de eventos de segurança da informação e a resposta a Incidentes de segurança da informação.

5.4. Procedimentos e Controles Adotados para Segurança da Informação e Cibernética

5.4.1. Controles de Segurança da Informação e Cibernética

Em vistas ao cumprimento das diretrizes de Segurança da Informação e Cibernética, o iFood Pago adota procedimentos e controles para reduzir a vulnerabilidade à Incidentes e para atender aos objetivos de segurança da informação e cibernética. Dentre eles:

(a) Autenticação, criptografia, prevenção e a detecção de intrusão;

(b) Prevenção de vazamento de informações por meio da realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra *softwares* maliciosos, estabelecimento de mecanismos de rastreabilidade, controles de acesso e de segmentação da rede de computadores, bem como armazenamento de cópias de segurança dos dados e das informações, conforme normativos vigentes;

(c) Desenvolvimento de sistemas de informação seguros e adoção de novas tecnologias empregadas nas atividades da Instituição;

(d) Existência de controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis;

(e) Controle, monitoramento e restrição de acesso aos ativos de informação à menor permissão e privilégios possíveis;

(f) Mitigação dos riscos de negócio e cibernéticos;

(g) Registro, análise da causa e do impacto, bem como controle dos efeitos de Incidentes relevantes para as atividades da Instituição, que abrange inclusive informações recebidas de empresas prestadoras de serviços a terceiros;

(h) Inventário dos cenários de crises cibernéticas relacionados aos Incidentes de segurança considerados nos testes de continuidade de serviços prestados;

(i) Testes de Intrusão internos e externos são realizados pela área de Segurança da Informação, no mínimo anualmente, com o intuito de garantir a eficácia dos processos, aferir as camadas de segurança e identificar vulnerabilidades;

(j) Elaboração de relatório anual de resposta a Incidentes no ambiente tecnológico da Instituição, o qual deve ser apresentado e aprovado pela Diretoria Estatutária, nos termos e dentro do prazo previsto na regulamentação aplicável;

(k) Classificação de Incidentes de segurança conforme a sua relevância de acordo com a classificação das informações envolvidas e o impacto na continuidade dos negócios;

(l) Avaliação periódica de empresas prestadoras de serviço que efetuam o tratamento de informações relevantes à Instituição e que oferecem serviços de processamento e armazenamento de dados e de computação em nuvem com o objetivo acompanhar o nível de maturidade de seus controles de segurança para a prevenção e o devido tratamento dos Incidentes;

(m) Utilização de critérios para a classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior;

(n) Adoção de processo de gestão de continuidade de negócios, conforme a Política de Continuidade de Negócios da Instituição;

(o) Definição de regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância, de forma que toda informação possua um proprietário e seja obrigatoriamente classificada recebendo os devidos controles para a confidencialidade desta, condizentes com as boas práticas de mercado e regulamentações vigentes;

(p) Implementação de ações para prevenir, identificar, registrar e responder Incidentes e crises de segurança que envolvam o ambiente tecnológico da Instituição e que possam ocasionar o comprometimento dos pilares de segurança da informação ou trazer risco reputacional, financeiro ou operacional;

(q) Implementação de ferramentas de prevenção e detecção de Incidentes, além de ferramentas de monitoramento de vulnerabilidades;

(r) Simulações de ataque coordenado entre as áreas de Tecnologia e Segurança da Informação para validar procedimentos relacionados a Incidentes;

(s) Adoção de mecanismos para a disseminação da cultura de segurança da informação e cibernética na Instituição, incluindo a implementação de programa de treinamentos obrigatórios para Foodlovers e Stakeholders, conforme aplicável;

(t) Prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos e o comprometimento da Diretoria Estatutária – considerando a ausência de Conselho de Administração – com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética;

(u) A composição das senhas devem seguir os requisitos de complexidade e ser únicas. Não devem ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar, em conformidade com o disposto no Procedimento de Gestão de Identidade e Acesso Lógico;

(v) Os acessos devem ser gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação observado o disposto no Procedimento de Gestão de Identidade e Acesso Lógico;

(w) Adoção de iniciativas para compartilhamento de informações sobre os Incidentes relevantes através de filiação em fóruns de discussão e pelo compartilhamento da plataforma de SIEM.

5.4.2. Processamento, Armazenamento de Dados e Computação em Nuvem

As contratações de serviços de terceiros para o processamento e armazenamento de dados, e de computação em nuvem seguem os requisitos de segurança estabelecidos pelo iFood Pago e pelo BACEN, avaliando a relevância do serviço contratado, criticidade, e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo serviço.

Os prestadores deste tipo de serviço que são contratados pela Instituição passam por avaliação de sua capacidade tecnológica e de segurança, a fim de garantir a conformidade das operações, confidencialidade, integridade, disponibilidade e capacidade de recuperação. O processo de avaliação, assim como o fluxo de compras, está descrito na Política de Compras vigente.

Os documentos relativos às análises realizadas para tomada de decisão relativa à contratação do prestador de serviço que atua com o processamento e armazenamento de dados e computação em nuvem resta arquivado pelo período de 10 (dez) anos, a contar do término da relação com o prestador de serviço.

5.4.3. Gestão de Acessos

As diretrizes de Gestão de Acessos do iFood Pago estão disciplinadas em documento próprio denominado "Procedimento de Gestão de Identidade e Acesso Lógico".

5.4.4. Gestão de Mudança

A Instituição zela pelo processo de gestão de mudança, que tem por objetivo assegurar que as mudanças realizadas nos ambientes de produção e homologação da Instituição sejam feitas de forma controlada, sendo avaliadas, planejadas, testadas, comunicadas, implementadas e documentadas, mitigando os riscos envolvidos nas mudanças de tecnologia em ambientes operacionais.

5.4.5. Cópias de Segurança e *Backup*

A Instituição possui diretrizes relacionadas à extração de cópias de segurança das informações, dos *softwares* e dos sistemas que podem ser observados no Procedimento de *Backup* e Restauração de Dados. É mantido o registro completo e exato das cópias de segurança, provendo documentação apropriada sobre os procedimentos de restauração da informação.

5.4.6. Gestão de Riscos e Incidentes de Segurança e Vulnerabilidades

O iFood Pago estabelece diretrizes e padrões a serem adotados a fim de garantir o atendimento às regulamentações aplicáveis e boas práticas de mercado, por meio da implementação de procedimentos de gerenciamento de riscos, em conformidade com a Declaração de Apetite ao Risco ("**RAS**") e normativos internos da Instituição.

Os riscos de segurança da informação e cibernética são identificados e acompanhados através de um processo de análise de vulnerabilidades, documentando em Procedimento de Gestão de Vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos

de informação, para associação dos níveis de proteção adequados.

O Procedimento de Resposta a Incidentes estabelece as diretrizes para o tratamento e a resposta adequada a cada tipo de Incidente de segurança da informação que possa impactar ativos/serviços de tecnologia da informação ou recursos computacionais da Instituição.

As informações relacionadas aos Incidentes de segurança da informação e cibernética possuem caráter confidencial, não devendo, em hipótese alguma, serem disponibilizadas às partes envolvidas e a terceiros que não os reguladores. A comunicação a terceiros, clientes e outras *Stakeholders* deve ser realizada em observância ao disposto no Manual de Comunicação para Gestão de Crises.

Todos os documentos referentes à Incidentes, incluindo coleta de evidências, devem ser arquivados pelo prazo mínimo de 5 (cinco) anos.

5.4.7. Política de Continuidade de Negócios

A Instituição possui documento específico intitulado "Política de Continuidade de Negócios" que visa garantir que existam planos de continuidade de negócios e recuperação de desastres que contemplem alocação de profissionais, os principais processos e ativos de tecnologia e negócio, bem como a possibilidade de elaboração de cenários de Incidentes a serem considerados em testes de continuidade dos serviços de pagamento prestados.

5.4.8. Segurança nas Operações

As atividades operacionais associadas ao processamento de informações confidenciais devem ser documentadas e disponibilizadas em portal corporativo para acesso dos Foodlovers que executam as atividades. Todas as diretrizes estão estabelecidas na Política de Segurança nas Operações.

5.4.9. Comunicação Eletrônica de Dados na Rede do Sistema Financeiro Nacional

A comunicação eletrônica de dados na RSFN, além de atender a regulamentação específica, prevê a aplicação dos seguintes controles:

(a) uso de múltiplos fatores de autenticação para o acesso administrativo aos ambientes Pix e Sistema de Transferência de Reservas ("**STR**");
(b) isolamento físico e lógico do ambiente Pix dos demais sistemas do Conglomerado, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de serviços de computação em nuvem contratados;
(c) isolamento físico e lógico do ambiente STR dos demais sistemas do Conglomerado, mantendo instância dedicada e apartada dos demais ambientes nos casos de uso de serviços de computação em nuvem contratados;
(d) monitoramento do uso de credenciais e certificados digitais, bem como estabelecimento de controles para a guarda dessas informações, especialmente as utilizadas no âmbito do Sistema de Pagamentos Instantâneos (SPI);
(e) implementação de mecanismos de validação da integridade fim a fim das transações pelo Conglomerado antes da assinatura digital das mensagens associadas, assegurando que os dados não tenham sido corrompidos ou manipulados durante o processo de geração dessas mensagens; e
(f) vedação do acesso de empresas prestadoras de serviços a terceiros às chaves privadas associadas a certificados digitais utilizados pela instituição para a assinatura de mensagens.

5.4.10. Gestão de Certificados Digitais

O iFood Pago realiza o monitoramento do uso de certificados digitais, incluindo a aplicação de controles para:

(a) Zelar pela rastreabilidade das informações;
(b) Assegurar a guarda das informações, abrangendo os controles de acesso físico e lógico a chaves privadas sob responsabilidade do Conglomerado;
(c) Evitar o compartilhamento indevido das chaves privadas associadas a certificados digitais do Conglomerado; e
(d) Zelar pela validação tempestiva de certificados revogados perante as autoridades certificadoras.

5.4.11. Proteção e Governança de Dados

As diretrizes de Proteção e Governança de Dados estão estabelecidas na "Política de Privacidade" e na "Política de Retenção e Governança de Dados" visando assegurar a privacidade e a segurança dos dados tratados no âmbito do iFood Pago.

5.4.12. Treinamento e Conscientização

O Programa de Treinamento e Conscientização em Segurança da Informação – que inclui treinamentos obrigatórios – observa um cronograma anual estabelecido com os tópicos relevantes a serem abordados em diferentes formatos de treinamento e conscientização, como, por exemplo:

(a) *Online* através da plataforma de conscientização vigente;

(b) *Online* e ao vivo através da plataforma de comunicação vigente, permitindo a interação com os participantes;

(c) Testes de *phishing* encaminhados ao e-mail dos colaboradores;

(d) Treinamentos específicos para atender a necessidade de um grupo de colaboradores; e

(e) Comunicados com dicas e materiais de conscientização divulgados aos colaboradores por meio dos canais oficiais de comunicação.

A comprovação da participação e reconhecimento do conteúdo é avaliada por meio de um questionário ou outro método adequado.

As evidências da execução do Programa de Treinamento e Conscientização em Segurança da Informação são armazenadas pela área de Segurança da Informação em local protegido.

5.4.13. Gestão de Consequências

Todos os colaboradores, fornecedores, parceiros e clientes que observarem quaisquer desvios em relação às diretrizes desta política deverão relatar o fato através do Canal de integridade iFood, disponível no site da empresa ou através do site https://www.canaldeintegridade.com.br/ifood/.

A Instituição garante a confidencialidade e anonimato das informações reportadas, bem como a não retaliação a denunciantes que estiverem agindo de boa-fé.

O descumprimento das diretrizes desta Política resultará na aplicação de medidas de

responsabilização, de acordo com o Código de Ética e Conduta iFood, bem como medidas administrativas ou legais cabíveis.

5.5. Contato com Autoridades por Incidentes

Nos casos em que haja necessidade de contato com autoridades por Incidentes relacionados à Segurança da Informação (por exemplo, no caso de suspeita de que a lei foi violada), ou a ocorrência de um Incidente, haverá primeiramente exposição dos fatos ao Comitê de Riscos e Compliance e deliberação da Diretoria Estatutária da Instituição, que definirão os responsáveis por esta comunicação e a forma como ela será feita, com base no Manual de Comunicação para Gestão de Crise e na Política do Canal da Integridade iFood.

Todos os Comitês têm suas diretrizes estabelecidas nos seus respectivos Regimentos Internos, disponíveis para conhecimento dos colaboradores no repositório corporativo.

5.6. Comprometimento da Alta Administração

A Alta Administração do iFood Pago – no caso da Instituição, a Diretoria Estatutária devido a ausência de Conselho de Administração – está comprometida com a segurança da informação e cibernética, especialmente através da constante transformação e aprimoramento da governança em ações relativas aos pilares e pela disponibilização de recursos compatíveis com a complexidade da organização.

5.7. Armazenamento e Divulgação da Política

As documentações relacionadas aos processos e procedimentos aqui estabelecidos estão arquivadas em ambiente seguro e permanecerão à disposição do órgão regulador pelo prazo mínimo de 5 (cinco) anos.

A divulgação desta Política para o público externo acontece por meio do nosso *website*. Já para o público interno, a Política está disponível no Portal de Governança Corporativa e os comunicados são compartilhados através dos nossos canais de comunicação por e-mail, sempre que houver atualizações.

6. RESPONSABILIDADES

6.1. **Foodlovers –** Os Foodlovers são responsáveis por:

(a) Observar e zelar pelo cumprimento da presente Política, estando ciente formalmente das diretrizes estabelecidas;

(b) Acionar o responsável pela área de Segurança da Informação, quando assim se fizer necessário, para consultas sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas;

(c) Cumprir as leis e normas que regulamentem os aspectos de propriedade intelectual e uso de dados;

(d) Zelar pela proteção dos dados confidenciais (dados pessoais, sensíveis, financeiros – inclusive dados de cartão, estratégicos ou protegidos por lei) da Instituição ou dados que estiverem sob sua responsabilidade durante o seu tratamento;

(e) Reportar à área de Segurança da Informação, de forma tempestiva, qualquer evento suspeito que possa comprometer o ambiente da organização ou que configure uma violação à presente Política;

(f) Sugerir, recomendar e verificar a implementação das melhores práticas de segurança em todos os processos de sua responsabilidade;

(g) Utilizar, para fins de trabalho, de forma responsável, profissional, ética e lícita, os ativos de

tecnologia da informação;

(h) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada; e

(i) Participar dos programas de conscientização visando compreender o papel da segurança da informação em suas atividades diárias.

6.2. **Diretoria Estatutária** – O Diretor Responsável por Segurança da Informação é responsável por:

(a) Cumprir e zelar pelo cumprimento desta Política e do disposto nas Resoluções do BACEN e CMN, conforme aplicável, que tratem sobre o tema incluindo as suas respectivas atualizações; e

(b) Atender e cumprir as demandas dos órgãos reguladores relacionadas à Segurança da Informação.

6.3. **Área de Segurança da Informação** – A área de Segurança de Informação é responsável por:

(a) realizar, anualmente ou sempre que necessário, a atualização dos normativos internos relacionados à Segurança da Informação, assegurando a sua conformidade com as leis e regulamentações aplicáveis;

(b) monitorar, analisar a criticidade de processos, manter e melhorar continuamente o seu SGSI documentado dentro do contexto das atividades dos negócios e dos riscos a que ela está sujeita.

(c) realizar avaliação de efetividade – para avaliação das áreas de riscos e auditoria interna ou externa – dos mecanismos de segurança através da realização de testes e monitoramentos;

(d) Elaborar relatório anual de incidentes do iFood Pago;

(e) Gerenciar, coordenar, orientar, avaliar e implantar as ações, controles, atividades e projetos relativos à Segurança da Informação, promovendo ações de interesse do iFood Pago, programas educacionais, de conscientização e de capacitação e de avaliação periódica de pessoal;

(f) armazenar, em local protegido, as evidências da execução do Programa de Treinamento e Conscientização em Segurança da Informação; e

(g) Criar mecanismos capazes de detectar, reportar e responder falhas ou incidentes de Tecnologia da Informação; e

(h) Zelar pela instalação e manutenção dos agentes de segurança da informação nos ativos de infraestrutura (servidores e estações de trabalho).

6.4. **Área de Tecnologia da Informação –** A área de Tecnologia da Informação é responsável por:

(a) Operacionalizar as normas e procedimentos relacionados a esta Política, por meio dos recursos de TI, zelando pela segurança, conforme orientação da área de Segurança da Informação; e

(b) Corrigir as vulnerabilidades identificadas nos ativos de tecnologia em ambientes de desenvolvimento, homologação e produção.

6.5. **Área de *Plataform Security*** – A área de *Platform Security* é responsável por estabelecer e gerenciar o Programa de Treinamento e Conscientização em Segurança da Informação.

6.6. **Área de Governança Corporativa** – A área de Governança Corporativa é responsável pela:

(a) condução do processo de revisão e aprovação de documentos submetidos pela área de Segurança da Informação; e

(b) disponibilização da versão atualizada e aprovada em portal corporativo.

6.7. **Comitê de Riscos e Compliance** – O Comitê de Riscos e Compliance é responsável, além de outras prerrogativas, por assessorar na implementação das ações de segurança da informação e riscos cibernéticos, com intuito de evidenciar a proteção dos dados, inclusive de cartão, em conformidade com o PCI-DSS, bem como com a legislação vigente.

7. DISPOSIÇÕES GERAIS

Esta Política terá vigência de **1 (um) ano**, devendo, findo o prazo, ser revista pela área responsável e aprovada pela **Diretoria Estatutária** das sociedades parte do iFood Pago, sem prejuízo de revisão e aprovação em período inferior, caso necessário.

Esta Política entra em vigor na data de sua aprovação, revogando documentos e versões anteriores que tratam do mesmo tema.

No caso de conflito entre as disposições desta Política e Estatuto/Contrato Social das sociedades parte do iFood Pago, prevalecerá o disposto nos referidos Estatutos/Contratos Sociais.

No caso de conflito entre as disposições desta Política e da legislação ou regulamentação vigentes, prevalecerá o disposto na legislação ou regulamentação, conforme aplicável.

8. HISTÓRICO DE ALTERAÇÕES E DE APROVAÇÕES

Código	Versão	Data de Aprovação	Itens Alterados	Descrição
iFP.POL	01	25/03/2020	N/A	Criação da Política
	02	05/10/2020	Todos os itens	Revisão da Política em atendimento à regulamentação de Circular BACEN nº 3.909/18.
	03	14/10/2021	Todos os itens	Alteração da Política para adaptação aos processos atuais e boas práticas.
	04	26/12/2022		Adaptação do processo de comunicação às autoridades conforme a Política de Consequências Inclusão da previsão de apresentação do relatório anual à Diretoria Estatutária até 31 de março de cada ano, em acordo com a Resolução 85 do Banco Central Inclusão da previsão de que empresas que oferecem serviços de processamento e armazenamento de dados e de computação em nuvem também serão avaliadas. Atualização das nomenclaturas, definições e do processo de aprovação de normativos da Zoop.
	05	02/01/2024		Atualização regulatória, com a substituição de normativos revogados pelos normativos vigentes do BCB; Atualização de nomenclaturas de times / áreas; Padronização geral de

				normativos da Zoop.
	06	25/03/2025		Revisão da Política em atendimento à regulamentação Resolução BCB nº 85/21, bem como para adaptação aos processos atuais e boas práticas. Adoção da política para todo o iFood Pago.
iFP.POL-011	07	25/09/2025		Readequação dos temas.
iFP.POL-011	07	30/03/2026	Atualização dos itens: 2.; 4 e 5.4.6 e inclusão dos itens 5.4.9 e 5.4.10	Atualização da Política em atendimento às regulamentações Resolução CMN 4.893/21 e BCB nº 85/21.

Esta Política foi aprovada em Reunião de Diretoria das sociedades parte do iFood Pago realizada em 30 de março de 2026