	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 1 / 17

1. OBJETIVO

Esta Política tem como objetivo estabelecer diretrizes relacionadas aos princípios e diretrizes na 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 da Segurança Cibernética.

2. REFERÊNCIAS

Esta Política tem como premissa atender as diretrizes estabelecidas na:

- (i) Resolução BCB nº 85/2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, e relacionadas;
- (ii) Resolução CMN nº 4.893, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil;
- (iii) ABNT NBR ISO 27001, norma padrão e a referência Internacional para a gestão da Segurança da informação.

3. ABRANGÊNCIA

Todos os sócios, diretores, gestores, administradores, colaboradores, parceiros, prestadores de serviço terceirizados e quaisquer demais pessoas físicas ou jurídicas contratadas ou outras entidades que participem, de forma direta ou indireta, das atividades e negócios da organização.


4. DEFINIÇÕES

Bacen ou BC: Banco Central do Brasil;

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 2 / 17

Confidencialidade: somente o usuário da informação, que esteja devidamente autorizado pelo gestor da informação, deve ter acesso às Informações respeitando os critérios de segregação de funções;

Adequação: 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;

Disponibilidade: garantir que as informações estejam sempre disponíveis para o usuário da informação;

Autenticidade: garantir a identidade de quem está enviando a Informação;

SIEM: Gerenciamento e Correlação de Eventos de Segurança

CMN: Conselho Monetário Nacional


PCI: Payment Card Industry

Comitê de Riscos e Compliance: grupo colegiado responsável por avaliar, deliberar e priorizar os temas mais críticos relacionados à Segurança da Informação e Riscos Cibernéticos.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 3 / 17

5. DIRETRIZES

Toda documentação relacionada ao processo aqui estabelecido são arquivados em ambiente seguro e permanecerão à disposição da autoridade reguladora pelo prazo mínimo de 5 (cinco) anos.

A divulgação deste documento para o público externo acontece por meio do nosso website. Já para o público interno, os comunicados são encaminhados por e-mail sempre que houver atualizações e o documento se encontra disponível para consulta em nossa plataforma de gestão de documentos, assim como outros documentos que compõem o Sistema de Gestão da Segurança da Informação (SGSI).

Alinhado com as estratégias internas de Tecnologia da Informação e com as boas práticas de Segurança da Informação, com base no modelo, natureza e complexidade dos negócios e das operações foram analisados padrões que se adequam às necessidades de proteção das informações da empresa.

Foram eleitas as normas NBR ISO IEC 27001 e 27002, bem como os padrões PCI e requerimentos Bacen, 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.

A estrutura organizacional montada 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 pertinente.

5.1. IMPLEMENTAÇÃO E OPERAÇÃO DA ÁREA DE SEGURANÇA DA INFORMAÇÃO


Com base no Sistema de Gestão da Segurança da Informação, a organização:

- i. Formula 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;

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 4 / 17


- ii. Implementa o plano para o tratamento de pontos de auditoria que estejam sob responsabilidade da área, para atender aos objetivos de controle identificados;
- iii. Implementa os controles selecionados para atender aos objetivos de controle;
- iv. Define como medir a eficácia dos controles ou grupos de controle selecionados e específica como essas medidas são usadas para avaliar a eficácia dos controles, visando produzir resultados comparáveis e reproduzíveis;
- v. Define 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
- vi. Implementa tecnologias para identificar tentativas e violações de segurança da informação, bem-sucedidas ou não, além de incidentes de segurança da informação;
- vii. Contribui com tecnologias e processos para detectar eventos de segurança da informação e assim prevenir os incidentes de segurança da informação pelo uso dos indicadores;
- viii. Realiza, a cada 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;
- ix. Gerencia as operações de Segurança da Informação;
- x. Gerencia os recursos de tecnologia sob sua custódia; e
- xi. Implementa 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.

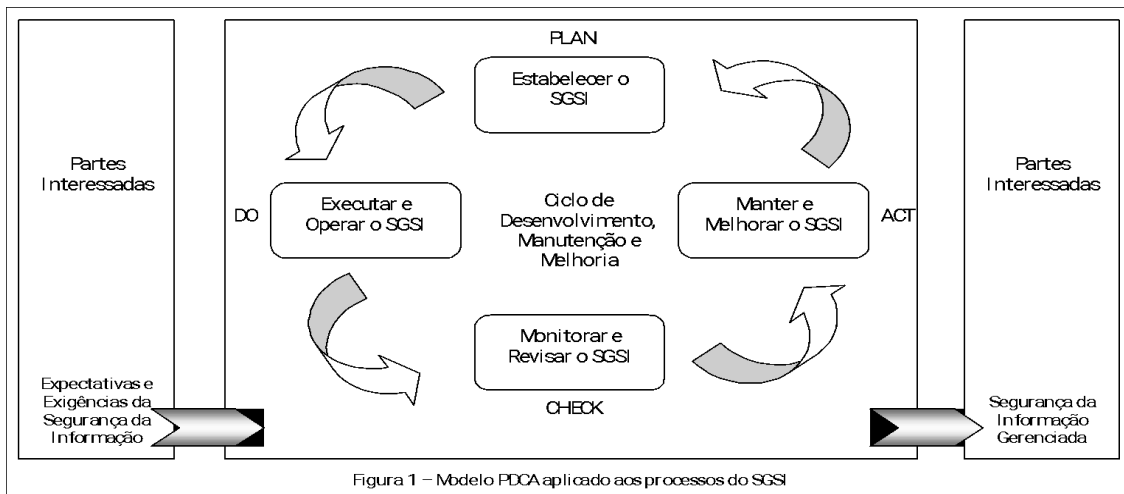
A área é responsável por monitorar, analisar a criticidade de processos, manter e melhorar continuamente o seu Sistema de Gestão da Segurança da Informação (SGSI) documentado dentro do contexto das atividades dos negócios e dos riscos a que ela está sujeita. Este processo está baseado no ciclo PDCA, conforme ilustrado na figura a seguir.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025
		Pág.: 5 / 17



5.2. PROCEDIMENTOS E CONTROLES ADOTADOS

5.2.1. 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, 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 organização 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 Guia de Procurement 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.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 6 / 17

5.2.2. CÓPIAS DE SEGURANÇA E BACKUP

A organização possui diretrizes relacionadas à extração de cópias de segurança das informações, dos softwares e dos sistemas que podem ser observados na Norma 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.

5.2.3. GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA

Os riscos de segurança da informação são identificados e acompanhados através de um processo de análise de vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos de informação, para associação dos níveis de proteção adequados.

O processo de respostas aos incidentes de segurança da informação está definido no Procedimento de Resposta a Incidentes, que estabelece diretrizes para garantir o tratamento e a resposta adequada a cada tipo de incidente de segurança da informação que possa impactar ativos/serviços de informação ou recursos computacionais da instituição.

5.2.4. PLANO DE CONTINUIDADE DE NEGÓCIOS

A organização possui documento específico intitulado “Plano de Gestão 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.

5.3. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades relacionados a esta Política estão estabelecidas abaixo:


5.3.1. PARTES INTERESSADAS

É dever das partes interessadas:

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 7 / 17

- i. Observar e zelar pelo cumprimento da presente Política, estando ciente formalmente das diretrizes estabelecidas e, quando assim se fizer necessário, acionar o responsável pela área de segurança da informação para consultas sobre situações que envolvam conflito com esta Política ou mediante a ocorrência de situações nela descritas;
- ii. Cumprir as leis e normas que regulamentem os aspectos de propriedade intelectual e uso de dados, como zelar pela proteção dos dados confidenciais (dados pessoais, sensíveis, financeiros – inclusive dados de cartão, estratégicos ou protegidos por lei) da organização ou dados que estiverem sob sua responsabilidade durante o seu tratamento;
- iii. Reportar à equipe de Segurança da Informação de forma tempestiva qualquer evento suspeito que possa comprometer o ambiente da organização ou que configure uma violação à Política de Segurança da Informação e Cibernética;
- iv. Sugerir, recomendar e verificar a implementação das melhores práticas de segurança em todos os processos de sua responsabilidade;
- v. Utilizar responsabilmente e para fins de trabalho, de forma profissional, ética e legal os ativos de tecnologia da informação;
- vi. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;
- vii. Compreender o papel da segurança da informação em suas atividades diárias e participar dos programas de conscientização.

5.3.2. DIRETOR RESPONSÁVEL POR SEGURANÇA DA INFORMAÇÃO


É dever do Diretor responsável por Segurança da Informação:

- i. Cumprir e zelar pelo cumprimento das diretrizes desta Política alinhada à Resolução do Banco Central do Brasil Nº 85/2021, bem como demais normativos internos correlatos e suas respectivas atualizações; e
- ii. Atender e cumprir as demandas dos órgãos reguladores relacionadas à Segurança da Informação.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 8 / 17

5.3.3. SEGURANÇA DA INFORMAÇÃO

É dever da área de Segurança da informação, 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.

5.3.4. GOVERNANÇA

Responsável pela gestão da documentação e apresentação para deliberação do Conselho de Administração ou no caso de inexistência deste, deliberação da Diretoria, bem como a publicação da versão atualizada em portal corporativo.

5.3.5. COMPLIANCE

Responsável por avaliar, de acordo com a metodologia e periodicidade que considerar adequada, a conformidade da Política de Segurança da informação e Cibernética, conforme legislação aplicável.

5.3.6. COMITÊ DE RISCOS E COMPLIANCE

É dever do Comitê de Riscos e Compliance, além de outras prerrogativas, 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 Programa PCI DSS, bem como com a legislação vigente.


Nos casos em que haja necessidade de contato com autoridades por irregularidades relacionadas 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 Executiva da instituição, que definirão os responsáveis por esta comunicação e a forma como ela será feita, com base 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 de normativos internos.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 9 / 17

5.4. ATIVOS DE SEGURANÇA DA INFORMAÇÃO

Para garantir a segurança das informações, os seguintes pilares devem ser respeitados e considerados em toda tomada de decisão:

- Confidencialidade – garantia de que as informações são acessadas somente por aqueles expressamente autorizados.
- Integridade – garantia de que as informações serão mantidas íntegras durante o ciclo de criação, processamento e descarte.
- Disponibilidade – garantia de que as informações estejam disponíveis sempre que necessário para o andamento de processos de negócio.

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 sua finalidade devidamente autorizada, sendo sujeitos a monitoramento e auditoria.

Todo ativo de informação de propriedade da organização 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. DIRETRIZES GERAIS


Com relação à segurança cibernética, são dispostas as seguintes diretrizes gerais:

- i. Proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 10 / 17

- ii. Adequada classificação das informações e garantia da continuidade do processamento destas, conforme os critérios e princípios indicados nos normativos específicos;
- iii. Garantia que os sistemas e dados sob nossa responsabilidade estão devidamente protegidos e estão sendo utilizados apenas para o cumprimento das nossas atribuições;
- iv. Zelo 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;
- v. Manutenção e gerenciamento de softwares antivírus, firewall e demais softwares de segurança instalados e atualizados e manutenção dos programas de computador instalados no ambiente; e
- vi. Atendimento às leis e normas que regulamentam as atividades realizadas.


Em vistas ao cumprimento das diretrizes acima elencadas, o objetivo de segurança cibernética prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. Com relação às medidas de segurança, são adotados procedimentos e controles para reduzir a vulnerabilidade a incidentes e para atender aos objetivos de segurança cibernética. Dentre eles:

- i. Autenticação, criptografia, prevenção e a detecção de intrusão;
- ii. Prevenção de vazamento de informações, 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 e armazenamento de cópias de segurança dos dados e das informações, conforme normativos vigentes;
- iii. Aplica os procedimentos e controles citados anteriormente, inclusive no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da organização;
- iv. Possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis.
- v. Controla, monitora, restringe o acesso aos ativos de informação à menor permissão e privilégios possíveis;
- vi. Contribui para a mitigação dos riscos de negócio e cibernéticos conforme a Política de Gerenciamento de Risco Operacional;

Público

Uso Interno

Confidencial


	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025
		Pág.: 11 / 17

- vii. Realiza o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da organização, que abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros;
- viii. Elabora inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços prestados e os testa anualmente para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes no ambiente tecnológico da organização, o qual deve ser apresentado e aprovado pela Diretoria Estatutária até 31 de março de cada ano, em acordo com a Resolução 85 do Banco Central;
- ix. Classifica os incidentes de segurança conforme sua relevância de acordo com a classificação das informações envolvidas e o impacto na continuidade dos negócios;
- x. Realiza a avaliação periódica de empresas prestadoras de serviço que efetuam o tratamento de informações relevantes à organização e que oferecem serviços de processamento e armazenamento de dados e de computação em nuvem. A avaliação tem como objetivo acompanhar o nível de maturidade de seus controles de segurança para a prevenção e o devido tratamento dos incidentes;
- xi. Possui critérios para classificação da relevância dos serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior;
- xii. Adota processo de gestão de continuidade de negócios, conforme a Política Corporativa de Continuidade de Negócios;
- xiii. Estabelece regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância. Toda informação possui um proprietário, é obrigatoriamente classificada e recebe os devidos controles que garantam a confidencialidade desta, condizente com as boas práticas de mercado e regulamentações vigentes;
- xiv. Realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o ambiente tecnológico da organização e que possam ocasionar o comprometimento dos pilares de segurança da informação ou trazer risco reputacional, financeiro ou operacional;
- xv. Implementa ferramentas de prevenção e detecção de incidentes, além de ferramentas de monitoramento de vulnerabilidades;
- xvi. Realiza simulações de ataque coordenado entre a equipe de TI e o time de Defensive para validar processos relacionados a incidentes.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 12 / 17

- xvii.** Adota mecanismos para disseminação da cultura de segurança da informação e cibernética na empresa, incluindo a implementação de programa de treinamentos obrigatórios para colaboradores, a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos e o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética; e
- xviii.** Adota iniciativas para compartilhamento de informações sobre os incidentes relevantes através de filiação em fóruns de discussão e pelo compartilhamento da plataforma de SIEM.]

5.6. COMPROMETIMENTO DA ALTA DIREÇÃO

O comprometimento da Alta Administração com a efetividade e a melhoria contínua desta Política, dos procedimentos e dos controles relacionados à segurança da informação e cibernética são percebidos através da constante transformação e aprimoramento da governança em ações relativas aos pilares mencionados anteriormente e pela disponibilização de recursos compatíveis com a complexidade da organização, avaliação e aprovação de Políticas, Normas e Procedimentos, dentre outras iniciativas.

5.7. TREINAMENTO E CONSCIENTIZAÇÃO


O Programa de Treinamento e Conscientização em Segurança da Informação é estabelecido e gerenciado pelo time *Plataform Security* do iFood. Um cronograma anual é estabelecido com os tópicos relevantes a serem abordados e podem ser adotados diferentes formatos de treinamento e conscientização, como por exemplo:

- Online através da plataforma de conscientização vigente;
- Online e ao vivo através da plataforma de comunicação vigente, permitindo a interação com os participantes;
- Testes de *phishing* encaminhados ao e-mail dos colaboradores
- Treinamentos específicos para atender a necessidade de um grupo de colaboradores; e
- Comunicados com dicas e materiais de conscientização divulgados aos colaboradores por meio dos canais oficiais de comunicação.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 13 / 17

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 pelo Segurança da Informação em local protegido.

5.8. REGISTROS E INFORMAÇÕES

As informações relacionadas aos incidentes de segurança da informação e cibernética são de caráter confidencial, não devendo, em hipótese alguma, serem disponibilizadas às partes envolvidas.

Todos os documentos referentes à investigação, incluindo coleta de evidências, devem ser arquivados pelo prazo mínimo de 10 (dez) anos.

5.9. NORMATIVOS DE SEGURANÇA DA INFORMAÇÃO

A equipe de Segurança da Informação mantém suas Políticas, Normas, Procedimentos e outras informações relevantes documentadas formalmente no repositório corporativo de normativos internos, bem como listados na seção 6 deste documento.

É papel do responsável pelo documento realizar a atualização do normativo pelo menos 1 (uma) vez ao ano, seguindo a diretriz corporativa de atualização de documentos estabelecida pela regulação.

Os documentos devem seguir a nomenclatura especificada abaixo:


POL – Políticas: devem ser classificados como Políticas todos os documentos que contêm diretrizes abrangentes e regras a respeito de um tema, considerando, principalmente, o teor regulatório e/ou legal envolvido. As Políticas devem ser aprovadas pelos Comitês Corporativos ligados aos seus respectivos temas, com envolvimento da diretoria na deliberação e a formalização da sua aprovação em ata de reunião.

NOR – Normas: devem ser classificados como Normas todos os documentos que contêm diretrizes e regras detalhadas sobre um determinado processo, sendo esses normativos normalmente associados com alguma Política previamente criada pela área. As Normas devem ser aprovadas pela

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 14 / 17

Diretoria ou pela Gerência da área responsável pelo documento, a depender do caso, sem necessidade de que passem pelos Comitês Corporativos.

PROD – Procedimentos: devem ser classificados como Procedimento todos os documentos que contêm instruções detalhadas sobre determinado processo. Os Procedimentos devem ser aprovados pela Gerência ou Coordenação da área responsável pelos documentos, devendo ser posteriormente enviados para ciência da Diretoria.

Outros documentos: Documentos que não se enquadrem nas categorias Políticas, Normas e Procedimentos (por exemplo: formulários, diagramas, etc) devem obedecer à nomenclatura vigente a ser estabelecida pelo time de Advisory, conforme a necessidade.

Os documentos que devem ser divulgados para toda a empresa devem ser encaminhados ao time de *Advisory* para revisão, que, por sua vez, encaminhará à equipe de Governança para aprovação e divulgação nas plataformas corporativas utilizadas na ocasião.

Já os documentos pertinentes somente à equipe de Segurança da Informação devem ser encaminhados somente ao time de *Advisory* para revisão e catalogação.

5.10. 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/>.

O descumprimento das diretrizes desta Política resultará na aplicação de medidas, de acordo com a Política do Canal de Integridade iFood, e na responsabilização dos agentes envolvidos.


5.11. AVALIAÇÃO DE EFETIVIDADE

A avaliação de efetividade é realizada pelo time de Segurança da Informação, onde, os testes e monitoramentos realizados, bem como os mecanismos de segurança são passíveis de avaliação das áreas de riscos e auditoria interna ou externa.

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025
		Pág.: 15 / 17

5.12. CONTATO COM GRUPOS ESPECIAIS

Com o objetivo de ampliar o conhecimento sobre as melhores práticas e nos mantermos atualizados com as informações relevantes sobre Segurança da Informação, estabelecemos contato com grupos especializados no tema.

Os contatos dos fornecedores de Segurança da Informação podem ser visualizados por meio dos links abaixo:

CERT BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. http://www.cert.br/
CVE Mitre	Registro, classificação e divulgação de vulnerabilidades técnicas https://cve.mitre.org/
Fornecedores de Segurança da Informação	Lista atualizada em posse do time de segurança responsável pelos fornecedores.

5.13. VIGÊNCIA DA POLÍTICA

Esta Política é revisada anualmente ou em período inferior caso seja necessária sua adequação.


Esta Política entra em vigor na data de aprovação pela Diretoria da Instituição e revoga quaisquer documentos em contrário.

6. DOCUMENTOS DE APOIO

Público

Uso Interno

Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025 Pág.: 16 / 17

Documentos	Objetivo
Norma Aquisição e Uso de Computadores	Estabelecer as competências, responsabilidades e atribuições dos envolvidos nos processos relacionados ao uso dos equipamentos e recursos disponibilizados pela Zoop.
Norma Classificação de Dados	Objetivo classificar as informações e estabelecer o tratamento de dados da Zoop, independentemente dos seus meios de armazenamento ou transmissão, com base em seu nível de sigilo, relevância, sensibilidade e potencial impacto ao negócio e ao titular dos dados.
Norma Desenvolvimento Seguro	Estabelecer os requisitos mínimos para o desenvolvimento seguro de sistemas, softwares e aplicações, visando a proteção dos dados e a redução dos riscos associados à segurança da informação e privacidade.
Norma Gestão de Hardening	Definir orientações quanto à criação e aplicação de hardening nos sistemas da Zoop.
Norma Segurança Física e do Ambiente	Estabelecer as diretrizes para que o acesso ao ambiente físico da Zoop seja controlado e monitorado, sendo concedido somente às pessoas autorizadas. Também faz parte deste normativo manter o processamento seguro das informações que envolvam equipamentos e recursos, por meio de ações preventivas e corretivas.
Norma Segurança nas Operações	Definir os requisitos para a operação correta e segura do processamento das informações, bem como a gestão dos recursos que garantam a segurança dessas informações.
Política Segurança da Informação e Cibernética	Estabelecer diretrizes que permitam à Zoop proteger seus ativos de informação, nortear a definição de normas e procedimentos específicos de Segurança da Informação e Cibernética.
Procedimento Gerenciamento de Testes de Invasão	Estabelecer o processo de execução das avaliações de segurança, especificando as áreas envolvidas e a periodicidade da execução dos testes de invasão, cujo objetivo é identificar, avaliar e remediar as falhas de segurança decorrentes das vulnerabilidades descobertas.
Procedimento Gestão de Identidade e Acesso Lógico	Definir as regras, controles e o fluxo que deve ser executado para prevenir acessos não autorizados aos sistemas de informação.
Procedimento Gestão de Regras de Firewall	Definir o fluxo e as responsabilidades para alterações nas regras dos firewalls e security groups relacionados ao ambiente escopo do PCI-DSS.
Procedimento Gestão de Riscos Cibernéticos e Privacidade	Estabelecer as diretrizes para o gerenciamento de Riscos em Segurança da Informação e Privacidade de Dados, em conformidade com a Política Corporativa de Gerenciamento de Risco Operacional.
Procedimento Gestão de Vulnerabilidades	Estabelecer as diretrizes para identificar falhas de segurança no ambiente de tecnologia e classificá-las por severidade, utilizando como referência a escala CVSS (Common Vulnerability Scoring System) para orientar a priorização das ações de correção.
Procedimento Resposta a Incidentes	Estabelecer uma lista de ações a serem realizadas no tratamento e resposta a incidentes de segurança da informação que minimizem o impacto no negócio e restaure serviços a normalidade o mais rápido possível.


7. REGISTRO DE ALTERAÇÕES

REVISÃO		ITEM ALTERADO	PRINCIPAIS ALTERAÇÕES
Nº	DATA		
01	25/03/2020	-	Elaboração 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	5.2.5 5.4 5.8	5.2.5 – Adaptação do processo de comunicação às autoridades conforme a Política de Consequências

(X) Público

() Uso Interno

() Confidencial

	POLÍTICA	Código: POL-007/25
	SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Data de Aprovação: 25/03/2025
		Pág.: 17 / 17

			<p>5.4. - Item VIII – 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</p> <p>5.4 - Item X – inclusão da previsão de que empresas que oferecem serviços de processamento e armazenamento de dados e de computação em nuvem também serão avaliadas.</p> <p>5.8 – Atualização das nomenclaturas, definições e do processo de aprovação de normativos da Zoop.</p>
05	02/01/2024	2; 5.2.1.2; 5.2.3.	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	Todos os itens	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.

8. FÓRUM DE APROVAÇÃO

A Política de Segurança da Informação e Cibernética é de responsabilidade da área de Segurança da Informação, em que é submetida ao Comitê de Riscos e Compliance para conhecimento e apresentada aos Diretores Executivos para aprovação, considerando a inexistência de Conselho de Administração.

Público

Uso Interno

Confidencial