

INFRAPAY

Tecnologia

POLÍTICA DE SEGURANCA CIBERNETICA

Conforme Resolução BCB no 85/2021 e Resolução CMN no 4.893/2021

Versão 01 | maio de 2026

IDENTIFICACAO DA INSTITUICAO

Razão Social: INFRAPAY TECNOLOGIA LTDA

Nome Fantasia: INFRAPAY

CNPJ: 66.689.331/0001-99

Endereço: Rua Visconde do Rio Branco, no 759, Sala 82 Anexo CLBC, Bairro Oficinas, Ponta Grossa/PR, CEP 84.036-030

E-mail de incidentes: contato@infrapay.tech

E-mail DPO: dpo@infrapay.tech

Site institucional: www.infrapay.tech

Diretor responsável pela Política: Marcelo Renato Leite de Andrade | Socio Administrador
| OAB/PR 106.406 | OAB/SC 55.771

1. INTRODUCAO

1.1. A presente Política de Segurança Cibernética tem como objetivo estabelecer princípios e diretrizes para a preservação e proteção das informações de Clientes, Colaboradores, Fornecedores, Parceiros, Partes Interessadas e da própria INFRAPAY TECNOLOGIA LTDA, contra ameaças e riscos relacionados à Segurança Cibernética.

1.2. Além disso, a Política visa implementar controles e procedimentos que reduzam a vulnerabilidade da INFRAPAY a incidentes, e regulamenta os requisitos para a contratação de serviços de processamento e armazenamento de dados, bem como de computação em nuvem, considerando a complexidade do modelo de negócios, das atividades e dos processos da Instituição.

1.3. A INFRAPAY implementa e mantém esta Política assegurando a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

1.4. Esta Política aplica-se a todos os Clientes, Colaboradores, Fornecedores, Parceiros, Partes Interessadas, Sócios e Administradores da INFRAPAY, independentemente de estarem vinculados a unidades físicas ou virtuais, ou da forma de acesso — local ou remoto — ao ambiente da Instituição.

1.5 Critérios adotados na elaboração desta Política

Na elaboração desta Política foram considerados:

- os produtos e serviços oferecidos pela INFRAPAY;
- o porte e o modelo de negócio da Instituição;
- a natureza das atividades realizadas;
- o perfil de risco da Instituição;
- a sensibilidade dos dados e informações coletados e armazenados sob responsabilidade da INFRAPAY.

1.6 Obrigações gerais de todos os envolvidos

Todos os envolvidos, direta ou indiretamente, na utilização ou suporte aos sistemas, a infraestrutura ou as informações da INFRAPAY devem:

- cumprir rigorosamente as normas e procedimentos estabelecidos nesta Política, assegurando o uso adequado das informações e dos sistemas associados;
- comunicar imediatamente as áreas responsáveis qualquer falha em dispositivos, serviços ou processos relacionados à Segurança Cibernética, para que ações corretivas sejam tomadas com agilidade — canal: contato@infrapay.tech;
- tratar as informações protegidas por esta Política como patrimônio estratégico da INFRAPAY, garantindo sua segurança, integridade e disponibilidade, conforme sua classificação e importância.

2. NORMAS REGULADORAS

2.1. Dentre as principais normas disciplinadoras do mercado financeiro no que tange à Segurança da Informação e Segurança Cibernética, destacam-se:

NORMA	EMENTA
-------	--------

Lei no 13.709/2018 (LGPD)	Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade.
Resolução CMN no 4.893/2021	Dispõe sobre a Política de Segurança Cibernética e requisitos para contratação de serviços de processamento, armazenamento de dados e computação em nuvem pelas instituições autorizadas pelo Banco Central do Brasil.
Resolução BCB no 85/2021	Dispõe sobre a política de segurança cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados e computação em nuvem para instituições de pagamento e corretoras autorizadas pelo Banco Central do Brasil.

3. DEFINICOES

3.1. Para fins desta Política, são considerados os seguintes conceitos:

TERMO	DEFINICAO
Administradores	Sócios administradores ou representantes legalmente constituídos da INFRAPAY, nomeados no Contrato Social ou em ato apartado devidamente registrado na Junta Comercial.
Reunião de Sócios	Reunião convocada para deliberar sobre assuntos previstos nesta Política, conforme art. 1.072 do Código Civil.
Amazon Web Services (AWS)	Plataforma de serviços de computação em nuvem amplamente utilizada para armazenamento, processamento e gestão de dados e sistemas.
Ativos	Qualquer forma de dados que geram informações, incluindo documentos impressos, sistemas, softwares, bancos de dados, arquivos digitais e dispositivos moveis.
BCB	Banco Central do Brasil.
Clientes / Usuários Finais	Pessoas físicas ou jurídicas que contratam e utilizam os produtos e/ou serviços da INFRAPAY.

Colaboradores	Empregados, prestadores de serviços sem vínculo empregatício, trainees e estagiários que atuam na INFRAPAY.
Comite de Segurança Cibernética	Comite formado por Colaboradores indicados pelos Administradores, responsável por deliberar sobre temas relacionados à Segurança Cibernética.
Diretor de Segurança Cibernética	Diretor designado para implementar, executar e manter esta Política e gerenciar o Plano de Ação e Resposta a Incidentes.
Fornecedores	Pessoas físicas ou jurídicas, públicas ou privadas, nacionais ou estrangeiras, que fornecem produtos ou prestam serviços a INFRAPAY.
Gerenciamento de Ativos	Práticas adotadas pela INFRAPAY para controlar Ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas, materiais e know-how).
Facilitador de tecnologia em Pagamentos	A INFRAPAY, que atua como facilitador de tecnologia de pagamentos.
Informações Sensíveis	Informações estratégicas para os negócios e operações da INFRAPAY, tangíveis por meio de transações, processamentos, bancos de dados e outros meios.
Parceiros	Pessoas físicas ou jurídicas, nacionais ou estrangeiras, que firmam contratos com a INFRAPAY para colaborar com seus negócios mediante retribuição.
Partes Interessadas	Colaboradores, sócios, Clientes, Fornecedores, Parceiros e a comunidade na qual a INFRAPAY está inserida.
Segurança Cibernética	Conjunto de tecnologias e processos destinados a proteger sistemas internos, computadores, redes e dados da INFRAPAY contra-ataques, danos, ameaças ou acessos não autorizados.

4. PRINCIPIOS

4.1. A INFRAPAY está comprometida em garantir a segurança e o tratamento adequado das informações. Para isso, adota práticas fundamentadas nos seguintes princípios:

PRINCÍPIO	DESCRICAO
Autenticidade	Garantia de identificar e autenticar Usuários, entidades, sistemas ou processos que tenham acesso às informações.
Confidencialidade	Garantia de que apenas pessoas autorizadas terão acesso às informações, e somente quando houver necessidade.
Inviolabilidade	Inviolabilidade da intimidade, honra e imagem de todos os Clientes e Colaboradores da INFRAPAY.
Eficiência	Garantir que a Política de Segurança Cibernética consiga atingir o objetivo de excelência na segurança de todos os dados presentes em seu banco de dados.
Disponibilidade	Garantia de que as informações estarão acessíveis as pessoas autorizadas sempre que necessário.
Integridade	Garantia de que as informações permanecerão exatas, completas e protegidas contra modificações indevidas.

5. DIRETRIZES

5.1. Para garantir os objetivos desta Política de Segurança Cibernética, os procedimentos seguirão as diretrizes abaixo:

(i) Cultura de Segurança Cibernética

A INFRAPAY implementa mecanismos para disseminar a cultura de Segurança Cibernética, incluindo:

- Programas regulares de capacitação: treinamentos periódicos para Colaboradores sobre boas práticas e riscos relacionados à Segurança Cibernética;
- Avaliação periódica de pessoal: monitoramento contínuo para garantir que todos compreendam e apliquem as diretrizes de Segurança Cibernética;
- Sensibilização organizacional: campanhas de conscientização para fortalecer o compromisso com a proteção de informações;
- Transparência: informações e orientações aos Usuários Finais sobre precauções no uso de produtos e serviços oferecidos pela INFRAPAY.

(ii) Controles de Acesso e Confidencialidade

- Garantir tratamento ético e sigiloso das informações, evitando acessos indevidos, modificações, destruições ou divulgações não autorizadas;
- Assegurar que o acesso dos Colaboradores seja pessoal, intransferível e limitado aos recursos necessários ao exercício de suas funções;
- Implementar mecanismos de gerenciamento de senhas e uso seguro de credenciais.

(iii) Classificação de Dados

Os dados e informações são classificados de acordo com sua relevância e sensibilidade, estabelecendo-se controles proporcionais ao risco de cada categoria.

(iv) Procedimentos de Segurança

A INFRAPAY implementa e mantém controles para reduzir vulnerabilidades, incluindo:

- autenticação e criptografia em todos os canais de acesso;
- prevenção e detecção de intrusão;
- prevenção de vazamento de informações (DLP);
- testes periódicos e varreduras para identificar vulnerabilidades;
- proteção contra softwares maliciosos (antimalware, EDR);
- rastreabilidade de informações e controle granular de acessos;
- segmentação da rede de computadores;
- manutenção de backups de dados e informações com testes de restauração.

(v) Gerenciamento Integrado de Incidentes

- Registrar, analisar causas e impactos de incidentes;
- Estabelecer parâmetros para avaliação da relevância e implicações de cada ocorrência;
- Controlar efeitos de incidentes, incluindo aqueles reportados por terceiros.
- Reportar imediatamente qualquer risco identificado ao canal contato@infrapay.tech.

(vi) Continuidade de Negócios

A INFRAPAY elabora e testa cenários de incidentes para garantir a continuidade dos serviços de pagamento prestados, incluindo hipóteses de indisponibilidade de fornecedores críticos e ataques cibernéticos de larga escala.

(vii) Fornecedores e Parceiros

A INFRAPAY define procedimentos e controles de prevenção e tratamento de incidentes para Fornecedores e Parceiros que manuseiem dados ou Informações Sensíveis ou que sejam críticos para a operação da Instituição, exigindo contratualmente a conformidade com esta Política.

(viii) Serviço de Nuvem

- A utilização de hospedagem externa e computação em nuvem depende do nível de sensibilidade dos dados e dos processos envolvidos, sendo baseada em análise de risco previa;
- Os serviços de processamento e armazenamento em nuvem (SaaS, IaaS, PaaS) devem possuir acesso seguro por interfaces HTTPS, autenticação segura e ambientes segregados;
- Os acessos devem ser controlados por logins e senhas individuais, previamente fornecidos e adequados a atividade de cada colaborador, com registros em trilhas de auditoria.

(ix) Propriedade Intelectual

- A INFRAPAY é proprietária ou custodiante responsável por toda informação criada, armazenada, transmitida, processada ou descartada por seus recursos ou por aqueles contratados em nuvem ou prestados por terceiros devidamente autorizados;
- É vetada aos Colaboradores a violação da propriedade intelectual da Instituição ou de terceiros, quer seja pelo uso indevido de imagens, textos, softwares, marcas ou pela cópia indevida de originais.

(x) Divulgação desta Política

Divulgação interna:

- compartilhamento integral com todos os Colaboradores no início do vínculo e a cada atualização;
- inclusão nos contratos com prestadores de serviços terceirizados;
- envio de atualizações anuais via e-mail corporativo;
- treinamentos sobre o conteúdo e as exigências desta Política.

Divulgação externa:

- publicação das diretrizes principais no site institucional www.infrapay.tech;
- disponibilização do resumo ao público geral de forma clara, direta e completa.

(xi) Gerenciamento desta Política

- monitoramento contínuo do cumprimento das diretrizes estabelecidas;
- implementação de melhorias nos processos de segurança;
- atualização anual e revisões extraordinárias conforme evolução das ameaças cibernéticas e alterações regulatórias.

6. GERENCIAMENTO DOS PROCESSOS DE SEGURANÇA CIBERNÉTICA

6.1. A fim de assegurar que todas as diretrizes sejam cumpridas e que os princípios de Segurança Cibernética sejam devidamente seguidos, a INFRAPAY adota políticas e procedimentos para os processos descritos a seguir.

6.2 Incidentes de Segurança

A INFRAPAY estabelece processos para identificação, tratamento e registro de incidentes de segurança, visando mitigar riscos e preservar a integridade, confidencialidade e disponibilidade das informações.

CANAL DE COMUNICACAO DE INCIDENTES

Incidentes ou suspeitas identificados por Colaboradores, Parceiros ou Fornecedores devem ser imediatamente comunicados via:

E-mail: contato@infrapay.tech

Os incidentes são classificados pelo risco e impacto nos negócios, sendo registrados, tratados e comunicados adequadamente.

6.3 Classificação de Relevância dos Incidentes

A INFRAPAY classifica os incidentes de segurança segundo sua relevância, a classificação das informações envolvidas e o impacto na continuidade dos negócios, conforme detalhado em manuais específicos. A classificação orienta a prioridade de resposta e os níveis de escalada.

6.4 Plano de Ação e Resposta a Incidentes

O Plano de Ação e Resposta a Incidentes contempla:

- ações para adequar as estruturas organizacional e operacional conforme esta Política;
- rotinas, procedimentos, controles e tecnologias para prevenção e resposta a incidentes;
- área responsável pelo registro e controle dos efeitos de incidentes relevantes;
- diretor designado responsável pela presente Política e execução deste Plano.

O Plano de Ação é aprovado pelos Administradores, documentado e revisado anualmente.

6.5 Relatório Anual de Resposta a Incidentes

O Relatório Anual de Resposta a Incidentes é elaborado com data-base de 31 de dezembro e:

- submetido ao Comitê de Segurança Cibernética, quando existente, ou aos Administradores na sua inexistência;
- apresentado aos Administradores até 31 de março do ano seguinte, conforme art. 8º, parágrafo 2º, II, da Resolução CMN nº 4.893/2021;
- revisado anualmente, incorporando as lições aprendidas do período.

6.6 Mecanismos de Rastreabilidade e Controle

A INFRAPAY adota mecanismos de rastreabilidade e controles específicos para garantir a segurança das Informações Sensíveis, incluindo:

- controles de rastreabilidade para todas as operações e transações realizadas na plataforma;
- gerenciamento específico de Informações Sensíveis em dispositivos autorizados;
- controles alinhados com a LGPD (Lei nº 13.709/2018);
- registro e monitoramento de acessos e alterações em dados sensíveis;
- trilhas de auditoria para operações críticas, permitindo a identificação da origem, alterações realizadas e responsáveis por cada operação.

6.7 Registro e Análise de Incidentes

A INFRAPAY mantém processo estruturado de documentação e análise de incidentes, que inclui:

- registro detalhado dos incidentes relevantes (data, hora, sistemas afetados, impacto estimado);
- análise de causa raiz e impacto nos negócios;
- avaliação dos efeitos nas atividades da Instituição;
- monitoramento das ações corretivas e preventivas;
- integração de informações de incidentes reportados por Fornecedores e Parceiros;
- documentação das medidas tomadas para resolução;
- métricas de impacto operacional e financeiro;
- lições aprendidas para prevenção futura.

6.8 Treinamentos e Conscientização em Segurança

A INFRAPAY desenvolve e mantém programa abrangente de conscientização em segurança que inclui:

- treinamentos regulares e obrigatórios sobre Segurança Cibernética para todos os Colaboradores;
- campanhas de conscientização com simulações práticas de ameaças (phishing simulado, engenharia social etc.);
- avaliações periódicas de conhecimento e efetividade dos treinamentos;
- comunicação clara sobre riscos e melhores práticas de segurança;
- orientação específica por função e nível de acesso às informações;

- guias práticos de segurança para Usuários Finais;
- atualizações sobre novas ameaças e medidas preventivas.

Os Administradores lideram pelo exemplo, promovendo cultura de segurança e melhoria contínua dos controles e processos. O programa é regularmente atualizado para abordar novos riscos e requisitos regulatórios.

6.9 Segurança em Novos Produtos e Serviços

A INFRAPAY avalia os riscos cibernéticos antes do lançamento de novos produtos e serviços, mudanças significativas em processos existentes, implementação de novas tecnologias e alterações em sistemas críticos. Cada mudança passa por avaliação de segurança (security review) e testes antes da implementação, garantindo que controles adequados sejam estabelecidos para proteger Clientes e dados.

6.10 Contratação de Serviços de Processamento e Computação em Nuvem

6.10.1 Seleção e Avaliação de Prestadores

A INFRAPAY realiza o processamento e armazenamento de dados e computação em nuvem através de prestadores de serviços rigorosamente avaliados, assegurando:

- conformidade com a legislação e regulamentação vigentes;
- acesso da INFRAPAY aos dados e informações processados;
- confidencialidade, integridade e disponibilidade dos dados;
- aderência dos Fornecedores as certificações exigidas (ex.: ISO 27001, SOC 2);
- disponibilidade de relatórios de auditoria independente contratada pelos Fornecedores;
- recursos adequados para monitoramento dos serviços prestados;
- segregação de dados dos Usuários por controles físicos ou lógicos;
- controles de acesso robustos para proteção das informações.

6.10.2 Avaliação de Risco na Contratação

Para cada contratação de serviço de nuvem, a INFRAPAY avalia:

- criticidade do serviço para a operação;
- sensibilidade dos dados processados;
- capacidade técnica e reputação do prestador;
- documentação dos procedimentos de avaliação;
- gerenciamento adequado e monitoramento contínuo dos serviços contratados.

6.10.3 Serviços de Computação em Nuvem

Os serviços de computação em nuvem disponíveis a INFRAPAY devem compreender um ou mais dos seguintes modelos:

- IaaS (Infraestrutura como Serviço): processamento e armazenamento de dados, infraestrutura de redes e recursos computacionais para implantação ou execução de softwares da INFRAPAY;
- PaaS (Plataforma como Serviço): implantação ou execução de aplicativos da INFRAPAY utilizando os recursos computacionais fornecidos pelo prestador;
- SaaS (Software como Serviço): execução de aplicativos via internet implantados pelo prestador com utilização de seus próprios recursos computacionais.

A INFRAPAY e o Fornecedor contratado compartilham a responsabilidade pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos serviços contratados, assegurando o cumprimento da legislação vigente.

6.10.4 Contratação no Exterior

Quando contratar serviços de nuvem no exterior, a INFRAPAY deverá observar:

- definição clara, antes da contratação, dos países e regiões específicas em que os serviços serão prestados, bem como dos locais onde os dados serão armazenados, processados e gerenciados;
- previsão de alternativas que assegurem a continuidade dos serviços de pagamento, caso ocorra a impossibilidade de manutenção ou a extinção do contrato.

6.10.5 Clausulas Obrigatórias nos Contratos de Nuvem

A INFRAPAY assegura que os contratos com Fornecedores e Parceiros de processamento e armazenamento em nuvem contenham:

- indicação dos países e regiões específicas em que os serviços serão prestados e onde os dados serão armazenados;
- adoção de medidas de segurança apropriadas para transmissão e armazenamento de dados;
- garantia de segregação dos dados e implementação de controles de acesso que protejam informações dos Usuários Finais;
- em caso de extinção do contrato: obrigatoriedade de transferência dos dados ao novo prestador ou a INFRAPAY, e exclusão dos dados armazenados após confirmação da integridade dos dados recebidos;
- garantia de acesso da INFRAPAY as informações, certificações, relatórios de auditoria e recursos de monitoramento dos serviços prestados;
- obrigação de notificar a INFRAPAY sobre qualquer subcontratação de serviços relevantes;
- obrigação de manter a INFRAPAY informada sobre limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação vigente;
- obrigação de conceder pleno e irrestrito acesso ao responsável pelo regime de resolução a contratos, documentação e informações sobre os serviços prestados.

6.11 Plano de Continuidade de Negócios (PCN)

No âmbito do Plano de Continuidade de Negócios (PCN), a INFRAPAY assegura:

- o tratamento de incidentes relevantes relacionados ao ambiente cibernético;

- procedimentos a serem adotados em caso de interrupção nos serviços de processamento, armazenamento de dados e computação em nuvem;
- a consideração de cenários de incidentes nos testes de continuidade dos serviços de pagamento prestados;
- a realização de testes periódicos do PCN, com registro e documentação de seus resultados;
- medidas para mitigar os efeitos de incidentes relevantes que causem interrupção nos serviços contratados;
- a definição do prazo para reinício ou normalização das atividades ou dos serviços relevantes interrompidos;
- inclusão de análise pos-incidente com registro e documentação das lições aprendidas;
- o estabelecimento e a documentação de critérios que definam uma situação de crise.

6.12 Mecanismos de Acompanhamento e Controle

A INFRAPAY implementa mecanismos de acompanhamento e controle para garantir a execução e a eficácia desta Política, do Plano de Ação e Resposta a Incidentes, e dos requisitos de contratação de serviços em nuvem, incluindo:

- definição de processos, testes e trilhas de auditoria;
- critérios detalhados para avaliação e monitoramento de Fornecedores contratados;
- métricas e indicadores apropriados de desempenho em segurança (KPIs de cibersegurança);
- identificação e correção de eventuais deficiências.

6.13 Arquivamento das Informações

A INFRAPAY armazena, em meio físico ou digital, pelo prazo mínimo de 5 (cinco) anos, as seguintes informações:

- o documento que formaliza esta Política de Segurança Cibernética;
- a ata de aprovação da Política e do Plano de Ação e Resposta a Incidentes pelos Administradores;
- o Plano de Ação e Resposta a Incidentes com as estratégias para tratamento e recuperação;
- o relatório anual de implementação e eficácia do Plano, incluindo resultados de testes;
- a documentação dos procedimentos para contratação de serviços relevantes de nuvem;
- a documentação detalhada sobre prestação de serviços no exterior, incluindo localização dos dados;
- os contratos firmados para prestação de serviços de nuvem;
- os dados, registros e informações gerados pelos mecanismos de acompanhamento e controle.

7. PAPEIS E RESPONSABILIDADES

AREA / FUNCAO	PRINCIPAIS RESPONSABILIDADES
Administradores	Avaliar, aprovar e revisar periodicamente esta Política; assegurar sua implementação e cumprimento integral; promover a melhoria contínua em Segurança Cibernética; incentivar a capacitação dos Colaboradores.
Comite de Segurança Cibernética	Submeter o relatório anual de implementação do Plano de Ação e Resposta a Incidentes para análise crítica; garantir que o relatório seja apresentado aos Administradores até 31 de marco do ano subsequente.
Diretoria de Segurança Cibernética	Implementar e manter esta Política; elaborar o relatório anual; monitorar indicadores de segurança; gerenciar acessos; garantir a continuidade dos negócios; promover treinamentos contínuos.
Area de Compliance	Identificar e monitorar regulamentações aplicáveis; analisar e executar ações de conformidade; apoiar treinamentos; participar ativamente do processo de revisão desta Política; garantir o compartilhamento das atualizações com todos os envolvidos.
Area de Tecnologia da Informação	Implementar medidas, controles, sistemas e tecnologias que minimizem a vulnerabilidade a incidentes; garantir a continuidade dos negócios; fornece orientações a Usuários Finais sobre boas práticas.
Consultoria Jurídica	Oferecer suporte e assessoria para assegurar que práticas e contratos estejam em conformidade com as normas e regulamentos vigentes, especialmente no que se refere a Segurança Cibernética.
Colaboradores	Ler, compreender e cumprir integralmente esta Política; encaminhar dúvidas a T.I.; notificar imediatamente qualquer evento que a viole ou que comprometa a segurança dos recursos computacionais da INFRAPAY.
Fornecedores e Parceiros	Cumprir integralmente esta Política e os Procedimentos publicados pela INFRAPAY; apresentar os documentos de

Políticas e Procedimentos a todos os seus próprios Colaboradores.

8. SANCOES E PENALIDADES

8.1. As violações desta Política, incluindo omissões ou tentativas não consumadas que exponham a INFRAPAY a riscos com repercussões reputacionais, sociais, políticas ou econômicas, estarão sujeitas as penalidades descritas no quadro abaixo:

SUJEITO	PENALIDADES APLICAVEIS
Colaboradores (CLT / Contrato)	Advertência por escrito; Suspensão não remunerada; Demissão por justa causa; Ação judicial civil e/ou criminal.
Colaboradores temporários e terceiros	Análise pelo Comitê de Riscos ou Administradores; Sanções conforme termos previstos no contrato; Rescisão contratual com apuração de perdas e danos.
Fornecedores e Parceiros	Notificação formal; Suspensão ou rescisão do contrato; Exigência de ressarcimento por danos causados; Ação judicial.

8.2. No caso de Colaboradores temporários ou terceiros, os Administradores analisarão a ocorrência e deliberarão sobre as sanções e punições aplicáveis, conforme os termos previstos no contrato.

9. DECLARACAO DE RESPONSABILIDADE

9.1. Os Colaboradores da INFRAPAY devem aderir formalmente a esta Política por meio do Termo de Adesão constante no Anexo I, comprometendo-se a agir em conformidade com suas diretrizes.

9.2. Os contratos firmados pela INFRAPAY com Fornecedores que envolvam Ativos de Informação relacionados a esta Política devem conter cláusula que assegure a proteção e a segurança das informações, com responsabilidade solidária em caso de incidente.

10. APROVACAO DESTA POLÍTICA

10.1. Esta Política é revisada anualmente, e seus efeitos só terão validade após aprovação pelos Administradores da INFRAPAY.

10.2. A Política de Segurança Cibernética é documentada e revisada no mínimo anualmente ou sempre que ocorrerem mudanças regulatórias relevantes, incidentes de grande impacto ou alterações significativas no modelo de negócios da Instituição.

HISTORICO DE VERSOES

Versão 01 - Maio/2026 | Versão inaugural da Política de Segurança Cibernética da InfraPay Tecnologia Ltda. (CNPJ 66.689.331/0001-99).

11. DIVULGACAO DESTA POLÍTICA

11.1. Esta Política será divulgada a todos os Colaboradores da INFRAPAY e empresas terceirizadas desde o início do relacionamento contratual, com atualizações anuais compartilhadas por e-mail corporativo.

11.2. A INFRAPAY disponibilizara em seu site institucional (www.infrapay.tech) um resumo ao público contendo as diretrizes principais desta Política de Segurança Cibernética, em linguagem clara e acessível.

APROVACAO E ASSINATURA

Esta Política foi aprovada pela Diretoria da InfraPay Tecnologia Ltda. e entra em vigor na data constante abaixo.

Marcelo Renato Leite de Andrade

Socio Administrador | InfraPay Tecnologia Ltda. | CNPJ 66.689.331/0001-99

OAB/PR 106.406 | OAB/SC 55.771

Ponta Grossa/PR, ____/____/2026

REVISÃO E ASSINATURA

Esta Política foi aprovada pela Diretoria da InfraPay Tecnologia Ltda. e entra em vigor na data constante abaixo.

Izildo Xavier Dos Reis Junior

Socio Administrador | InfraPay Tecnologia Ltda. | CNPJ 66.689.331/0001-99

CPF 095.548.339-54

Curitiba/PR, ____/____/2026

ANEXO I - TERMO DE ADESAO A POLÍTICA DE SEGURANCA CIBERNETICA

TERMO DE ADESAO E CIENCIA
INFRAPAY TECNOLOGIA LTDA CNPJ 66.689.331/0001-99
Política de Segurança Cibernética - Versão 01 maio/2026

Eu, _____, brasileiro(a), portador(a) do CPF/MF sob o no _____, residente e domiciliado(a) na _____, declaro ter pleno conhecimento da Política de Segurança Cibernética da INFRAPAY TECNOLOGIA LTDA, publicada internamente, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da Instituição.

Declaro, ainda, ter ciência de que:

- devo cumprir rigorosamente todas as normas e procedimentos estabelecidos nesta Política;
- em caso de incidente de segurança ou ameaça de incidente, devo comunicar imediatamente a área responsável por meio do e-mail contato@infrapay.tech;
- o descumprimento desta Política sujeita-me as penalidades previstas na Seção 8, conforme aplicável a minha relação com a INFRAPAY.

Ponta Grossa/PR, ____ de _____ de 2026.

Assinatura
Nome: _____
Cargo / Função: _____
CPF: _____

ANEXO II - DIVULGAÇÃO DAS LINHAS GERAIS DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Introdução

A Política de Segurança Cibernética da INFRAPAY estabelece princípios e diretrizes para proteger informações de Clientes, Colaboradores, Parceiros e Partes Interessadas. Através desta Política, a INFRAPAY adota procedimentos e controles para reduzir a vulnerabilidade a incidentes e garantir a Segurança Cibernética, com o comprometimento da alta administração em melhorar continuamente as práticas de segurança.

A Política aplica-se a todos os envolvidos, exigindo que sigam procedimentos de segurança e relatem incidentes imediatamente.

Princípios

A Política baseia-se nos princípios de Autenticidade, Confidencialidade, Inviolabilidade da intimidade e honra de Clientes e Colaboradores, Eficiência, Disponibilidade e Integridade das informações.

Gerenciamento da Segurança Cibernética

A INFRAPAY adota controles de segurança física, monitoramento de incidentes e testes regulares, estabelecendo processos para identificação, tratamento e registro de incidentes de segurança.

A INFRAPAY conta com um Plano de Ação e Resposta a Incidentes, que abrange o registro, a análise de causas e impactos, o controle dos efeitos de incidentes significativos e diretrizes claras para simulação de cenários nos testes de continuidade dos serviços de pagamento.

A classificação de dados e informações quanto a sua relevância, aliada a definição de parâmetros para avaliação da relevância de incidentes, é essencial para garantir a Segurança Cibernética e assegurar uma resposta eficaz.

A disseminação da cultura de Segurança Cibernética é promovida por meio de programas de capacitação, avaliação periódica de pessoal e comunicação sobre precauções de segurança aos Usuários Finais.

Contratação de Serviços de Processamento e Computação em Nuvem

A INFRAPAY assegura que todas as diretrizes relacionadas a contratação de serviços de processamento, armazenamento de dados e computação em nuvem, no Brasil ou no exterior, estejam alinhadas com sua Política e procedimentos, adotando práticas de governança corporativa proporcionais a relevância do serviço contratado e aos riscos associados.

A capacidade dos prestadores de serviços é rigorosamente validada para garantir conformidade legal, confidencialidade, integridade, disponibilidade e recuperação dos dados, aderência às certificações exigidas, segregação dos dados dos Clientes e qualidade dos controles de acesso.

Canal de Comunicação

CONTATO PARA INCIDENTES E DÚVIDAS

E-mail de incidentes: contato@infrapay.tech

E-mail DPO / Privacidade: dpo@infrapay.tech

Site institucional: www.infrapay.tech

Endereço: Rua Visconde do Rio Branco, no 759, Sala 82 Anexo CLBC, Bairro Oficinas, Ponta Grossa/PR, CEP 84.036-030

Telefone: (47) 9653-8777

Responsável: Marcelo Renato Leite de Andrade | OAB/PR 106.406 | OAB/SC 55.771