

**INGRUPO****POLÍTICA DE SEGURANÇA CIBERNÉTICA****Dezembro de 2020**

<b>Título</b>	Política de Segurança Cibernética
<b>Número de referência</b>	0002
<b>Número de versão</b>	V 01
<b>Status</b>	Aprovada
<b>Aprovador</b>	CEO e VP
<b>Data da aprovação</b>	04/12/2020
<b>Data da próxima revisão</b>	03/12/2021
<b>Área responsável</b>	Presidência da It's Pay
<b>Normas externas e documentos relacionados</b>	Resolução CMN 4.658/2018
<b>Normas internas relacionadas</b>	Política de Risco Operacional

<b>Versão</b>	<b>Motivo</b>	<b>Data</b>	<b>Autor</b>	<b>Aprovador</b>
1	Implementação	04/12/2020	Área de Riscos	CEO e VP

## Sumário

<b>I - Objetivo .....</b>	<b>3</b>
<b>II - Abrangência.....</b>	<b>3</b>
<b>III - Base Legal.....</b>	<b>3</b>
<b>IV - Programa de Segurança da Informação .....</b>	<b>3</b>
<b>V - Segurança Cibernética .....</b>	<b>3</b>
<b>VI - Plano de Monitoramento e Resposta a Incidentes .....</b>	<b>4</b>
<b>VII - Proteção contra softwares maliciosos .....</b>	<b>4</b>
<b>VIII - Controles de acesso e segmentação da rede de computadores .....</b>	<b>4</b>
<b>IX - Manutenção de cópias de segurança dos dados e das informações .....</b>	<b>4</b>
<b>X - Desenvolvimento de sistemas e adoção de novas tecnologias .....</b>	<b>4</b>
<b>XI - Responsabilidade e comunicação .....</b>	<b>5</b>

## **I - Objetivo**

Estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação cibernética e promover a melhoria contínua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com o ambiente cibernético, assim como possibilitar a manutenção da confidencialidade, da integridade e da disponibilidade das informações sob responsabilidade do INGRUPO.

## **II - Abrangência**

Todos os administradores (Diretoria e demais gestores) e colaboradores das empresas ligadas e controladas pelo INGRUPO (In Mais, In Mais Prêmios, It's Pay e Bank10) doravante denominadas "INGRUPO" ou "Holding".

## **III - Base Legal**

O INGRUPO segue os requerimentos da Resolução CMN 4.658, que dispõe sobre a política de segurança cibernética e 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.

## **IV - Programa de Segurança da Informação**

Os controles de segurança cibernética fornecem a base do Programa de Segurança da Informação, estabelecem as regras para proteger o ambiente de TI e estão amparados nos seguintes pilares de governança e melhores práticas:

- 1.1 Garantir a segurança e a confidencialidade das informações de clientes, parceiros, fornecedores e empregados;
- 1.2 Proteger contra ameaças ou riscos à segurança dessas informações;
- 1.3 Proibir o acesso não autorizado ou o uso de informações que possam prejudicar os clientes ou empregados;
- 1.4 Armazenar, transportar e descartar adequadamente informações de clientes, parceiros, fornecedores e empregados;
- 1.5 Informar os empregados sobre suas responsabilidades de proteger as informações sob custódia do INGRUPO e a segurança dos sistemas;
- 1.6 Garantir que os prestadores de serviços terceirizados relevantes cumpram nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;
- 1.7 Cumprir todos os requisitos de notificação do cliente para proteção das informações.

## **V - Segurança Cibernética**

A fim de reduzir a vulnerabilidade aos incidentes e cumprir os objetivos da segurança cibernética, a Área de Segurança da Informação da It's Pay é responsável pela criação, proposição, administração e supervisão de políticas e normas concebidas para garantir que os riscos sejam identificados e gerenciados dentro de tolerâncias corporativas definidas, incluindo a prevenção, detecção, contenção e correção de violações de segurança cibernética.

- 1.1 Os programas são documentados e atualizados anualmente para garantir a conformidade contínua com os requisitos regulamentares. O INGRUPO implementa a autenticação de usuários em plataforma tecnológica, requisitos de criptografia de dados sensíveis, prevenção e detecção

de intrusão e de vazamento de informações, além da realização de testes e varreduras para detecção de vulnerabilidades;

1.2 A Norma de Gerenciamento de Identidade e Autenticação tem como principal objetivo o gerenciamento de identidades digitais para usuários, sistemas e processos, bem como na verificação de identidades que acessam recursos de TI do INGRUPO.

## **VI - Plano de Monitoramento e Resposta a Incidentes**

A identificação e a eliminação tempestiva de vulnerabilidades de tecnologia são fundamentais para garantir a integridade do ambiente dos processos de negócios. O Plano visa a descoberta de vulnerabilidades aplicáveis ao INGRUPO, define processos que combinem o monitoramento contínuo para identificar os recursos afetados e a avaliação de riscos para determinar a priorização para a correção.

1.1. São estabelecidas as medidas de preparação, identificação, contenção, erradicação, recuperação e gestão do conhecimento gerado, além da definição de requisitos de monitoramento e resposta e responsabilidades.

## **VII - Proteção contra softwares maliciosos**

Estão definidos os requisitos de controle de detecção e prevenção para impedir que códigos maliciosos sejam executados e se infiltrem na rede do INGRUPO. Os mecanismos de proteção contra códigos maliciosos incluem, por exemplo, o monitoramento de atividades de *endpoints*.

1.1 O INGRUPO captura eventos relevantes para a identificação de possíveis incidentes de segurança cibernética (aqueles resultantes de atividades de intenção maliciosa). Os eventos são capturados e analisados pelo Centro de Operações de Segurança (*SOC – Security Operations Center*) da It's Pay e utiliza serviços e ferramentas para monitorar e analisar os dados e alertas.

## **VIII - Controles de acesso e segmentação da rede de computadores**

O programa de Gerenciamento de Identidade e Acesso implementa padrões e controles de acesso em toda a infraestrutura e aplicativos, especialmente aqueles que contêm informações de clientes. Esses controles são projetados para autenticar usuários, permitir acesso autorizado, garantir procedimentos administrativos consistentes, manter a segregação de funções e garantir atualizações tempestivas por meio de processos de inclusão, exclusão ou transferência nos sistemas do INGRUPO.

## **IX - Manutenção de cópias de segurança dos dados e das informações**

O backup operacional abrange proteção de dados em nível de arquivo, retenção de dados e recuperação de arquivos para atender aos requisitos de recuperação operacional e inclui backup de dados, restauração e validação de backup e recertificação.

## **X - Desenvolvimento de sistemas e adoção de novas tecnologias**

O INGRUPO estabelece os requisitos de controle para o desenvolvimento de tecnologia, incluindo mudanças de software e configuração, independentemente da estrutura ou do modelo do ciclo de vida de desenvolvimento de software seguido pela equipe.

1.1. Esta norma se aplica aos softwares desenvolvidos pela It's Pay Tecnologia S/A, incluindo alterações de configuração, e aos desenvolvedores associados a esse desenvolvimento.

## **XI - Responsabilidade e comunicação**

O cumprimento desta Política é de responsabilidade de todos os colaboradores e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

1.1. A alta Administração do INGRUPO, compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política. Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicadas imediatamente para a Direção da It's Pay.

1.2. O treinamento em segurança cibernética é obrigatório para todos os empregados. O treinamento é baseado nas políticas e normas de segurança cibernética e é complementado por um programa de conscientização.