Fevereiro de 2022

Título	Política de Segurança Cibernética
Número de referência	006
Número de versão	V 02
Status	Aprovada
Aprovador	CEO
Data da aprovação	25/02/2022
Data da próxima revisão	25/02/2024
Área responsável	Presidência da It's Pay
Normas externas e documentos relacionados	Resolução CMN 4.658/2018
Normas internas relacionadas	Política de Risco Operacional

REVISÃO		**ÁREA RESPONSÁVEL**	**APROVADOR**	**DESCRIÇÃO DA ALTERAÇÃO**
Versão	**DATA**			
01	04/12/2020	Área de Riscos	CEO e VP	Implementação
02	25/02/2022	Área de Riscos	CEO	Revisão periódica

Sumário

1. 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.

2. 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”.

3. 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.

4. 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:

4.1. Garantir a segurança e a confidencialidade das informações de clientes, parceiros, fornecedores e empregados;

4.2. Proteger contra ameaças ou riscos à segurança dessas informações;

4.3. Proibir o acesso não autorizado ou o uso de informações que possam prejudicar os clientes ou empregados;

4.4. Armazenar, transportar e descartar adequadamente informações de clientes, parceiros, fornecedores e empregados;

4.5. Informar os empregados sobre suas responsabilidades de proteger as informações sob custódia do Ingrupo e a segurança dos sistemas;

4.6. Garantir que os prestadores de serviços terceirizados relevantes cumpram nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;

4.7. Cumprir todos os requisitos de notificação do cliente para proteção das informações.

5. 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.

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.

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.

6. 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.

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

7. 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*.

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.

8. 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.

9. 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.

10. 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.

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

11. 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.

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.

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.