# POLÍTICA DE SEGURANÇA CIBERNÉTICA - CONGLOMERADO PRUDENCIAL MAGALUPAY

## CONTROLE DE ALTERAÇÕES

| Revisão | Data | Local da Revisão | Descrição |
|---|---|---|---|
| 0 | 12/05/2021 | - | Emissão inicial |
| 1 | 25/07/2022 | Toda a Política | Revisão Geral da Política; Alteração do *e-mail* da Gerência de Segurança da Informação para <seginfo@magalupay.com.br>. |
| 2 | 27/09/2023 | Toda a Política | Revisão Geral da Política, com alteração nos itens 2, 3, 4, 5.5, 5.14, 6.3, 6.4 e 7. |
| 3 | 27/12/2023 | Itens 3 e 4.3 | Alteração nos itens 3 e 4.3. |
| 4 | 27/08/2024 | Toda a Política | Ajuste nos itens 2, 3, 4.2, 4.6, 5.2 e 5.9. |
| 5 | 14/03/2025 | Itens 2 a 7 | Ajuste nos itens 2, 3, 4.4, 4.5, 5.16, 7. |
| 6 | 01/07/2026 | Toda a Política | Ajuste nos itens 2, 3, 4.1, 4.2, 4.5, 4.6, 4.7, 5.2, 5.12 e 7.<br>Itens incluídos 4.3, 4.6.1, 4.6.2, 5.3, 5.8 e 8. |

## LISTA DE DISTRIBUIÇÃO

| Função |
|---|
| Todos os administradores, colaboradores, prestadores de serviços e parceiros das empresas sob o Conglomerado Prudencial MagaluPay. |

## LISTA DE TREINAMENTO

| Áreas funcionais |
|---|
| Todos os administradores, colaboradores, prestadores de serviços e parceiros das empresas sob o Conglomerado Prudencial MagaluPay. |

**Elaborado/Revisado por:**
Gerência de Segurança da Informação
Diretoria de *Compliance*, Integridade e PLD
Diretoria Jurídica

## 1. OBJETIVO

Garantir a proteção e a manutenção da integridade, disponibilidade e confidencialidade de todas as informações e sistemas sob responsabilidade do Conglomerado Prudencial MagaluPay (MagaluPay Instituição de Pagamento S.A. e MagaluPay - Sociedade de Crédito, Financiamento e Investimento S.A.), inclusive em ambientes de nuvem. O foco é instituir diretrizes de contratação segura e atuar na prevenção, detecção e redução de vulnerabilidades e incidentes cibernéticos.

Nosso objetivo é garantir a segurança das informações e dos serviços que oferecemos, adotando critérios rigorosos na contratação de parceiros e prestadores de serviços. Também atuamos de forma contínua na prevenção, identificação e resposta a vulnerabilidades e incidentes cibernéticos, proporcionando um ambiente financeiro mais seguro, confiável e protegido.

## 2. PRINCÍPIOS DE SEGURANÇA

Nossas ações são norteadas por três pilares fundamentais da Segurança da Informação:

- **Confidencialidade:** Garantir que as informações sejam de conhecimento exclusivo de pessoas especificamente autorizadas.
- **Integridade:** Assegurar que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais.
- **Disponibilidade:** Garantir que as informações e sistemas estejam disponíveis a todas as pessoas autorizadas quando necessário.

## 3. GOVERNANÇA

A governança é exercida por meio de responsabilidades bem definidas entre os órgãos estatutários e comitês:

- **Diretoria Executiva e Estatutária:** Responsável por avaliar, aprovar e prover os recursos necessários para o cumprimento da política, integrando o risco cibernético ao pilar estratégico de tomada de decisão.
- **Comitê Executivo:** Delibera sobre temas críticos, riscos muito altos e aprova eventuais exceções operacionais.
- **Comitê de Tecnologia e Segurança Cibernética:** Atua como fórum de primeira instância para acompanhar KRIs/KPIs, tendências, incidentes e o nível de aderência regulatória (Bacen e PCI-DSS).

## 4. GESTÃO DE RISCOS CIBERNÉTICO

O gerenciamento de riscos cibernéticos é um processo contínuo integrado à governança corporativa. A área de Segurança da Informação é responsável por identificar, classificar, monitorar e governar esses riscos até sua mitigação ou redução a níveis aceitáveis. Adicionalmente, qualquer desenvolvimento, aquisição ou grande mudança em sistemas que envolva dados produtivos ou pessoais passa por uma avaliação formal de riscos antes de sua implementação.

## 5. PROTEÇÃO DAS INFORMAÇÕES

Implementamos controles técnicos rigorosos para blindar o ecossistema tecnológico:

- **Autenticação:** Uso obrigatório de Duplo Fator de Autenticação (MFA) e aplicação do princípio do privilégio mínimo para concessão de acessos.
- **Segurança de Credenciais:** Políticas de senhas com critérios de alta complexidade, limite de tentativas de login e tempo máximo de expiração.
- **Proteção de Ambientes Críticos:** Isolamento físico e lógico de ambientes regulados (como Pix e STR), com proibição do acesso de terceiros a chaves privadas corporativas.
- **Controle de Dados:** Rastreabilidade por meio de trilhas de auditoria automatizadas (logs) integradas a uma plataforma de monitoramento em tempo real (SIEM).

## 6. GESTÃO DE INCIDENTES

Contamos com uma Política e um Plano de Resposta a Incidentes formalmente instituídos, que orientam nossas ações desde a detecção até a completa resolução de eventos cibernéticos. Possíveis ataques são identificados por barreiras técnicas (como firewalls, antivírus e VPNs) e pelo monitoramento proativo externo.

Em caso de qualquer suspeita ou confirmação de anormalidade, o processo de triagem e investigação é iniciado imediatamente. Incidentes classificados como relevantes que possam impactar a continuidade dos negócios ou envolver dados pessoais , são prontamente reportados à Diretoria Executiva, à área de Privacidade (DPO) e, em total conformidade com as normas vigentes, comunicados tempestivamente ao Banco Central do Brasil.

## 7. GESTÃO DE TERCEIROS

Asseguramos que todos os prestadores de serviços, fornecedores e parceiros de negócios tomem

total ciência e cumpram as nossas diretrizes de segurança cibernética. O relacionamento com esses parceiros segue um ciclo de vida rigorosamente estruturado:

- **Planejamento e Due Diligence:** Realizamos avaliações minuciosas antes de qualquer contratação para analisar e validar os controles de segurança do parceiro.
- **Formalização Contratual:** Todos os contratos possuem cláusulas obrigatórias e específicas de segurança da informação, em total conformidade com a legislação vigente.
- **Ciência das Políticas:** Asseguramos que todos os parceiros tomem total ciência e cumpram as diretrizes da nossa Política de Segurança da Informação, além de nossas regras de segurança cibernética.

## 8. CONSCIENTIZAÇÃO E TREINAMENTO

Buscamos fomentar de forma ativa a cultura de segurança cibernética. Para isso, asseguramos que todos os colaboradores, parceiros, terceiros, administradores tomem total ciência sobre as nossas políticas de segurança. Realizamos treinamentos obrigatórios anuais (ou sempre que a política sofrer atualizações importantes) para todos os colaboradores, além de campanhas periódicas e comunicações em canais internos que mantêm o tema presente no dia a dia da organização.

## 9. CONTINUIDADE DE NEGÓCIOS

Garantimos a resiliência operacional por meio de um Plano de Continuidade de Negócios robusto, composto por análises de impacto (BIA), planos de recuperação de desastres e gestão de crises. Para sustentar essa solidez, asseguramos que todos os sistemas desenvolvidos internamente atendam rigorosamente aos padrões de segurança da informação e às melhores práticas de mercado e corporativas. Além disso, nossa infraestrutura possui contingenciamento de energia (no-breaks), redundância em nuvem e zonas distintas, bem como rotinas automatizadas de backup.

## 10. DISPOSIÇÕES GERAIS

### 10.1 Aplicabilidade

Esta política é de aplicação obrigatória e irrestrita, possui vigência imediata a partir de sua aprovação pelas Diretorias responsáveis e é revisada anualmente (ou sempre que houver necessidade motivada por alterações regulatórias ou evoluções tecnológicas), assegurando que nossa postura de defesa cibernética permaneça robusta e atualizada.