Versão vigente: 08/2026
Elaborada/revisada por: Acácio Roboredo (Diretor de Compliance)

Política de Segurança da Informação e Segurança Cibernética

LAPB Gestão de Recursos Financeiros Ltda.

08.2026

1. INTRODUÇÃO

A Política de Segurança da Informação e Segurança Cibernética ("Política") estabelece as diretrizes a serem seguidas pela LAPB Gestão de Recursos Financeiros Ltda. ("LAPB" ou "Gestora") para garantir a proteção das informações sob sua posse.

A segurança da informação está relacionada à proteção de um conjunto de dados, de modo a preservar o valor que possuem para um indivíduo ou organização, e apoia-se nos atributos de confidencialidade, integridade e disponibilidade. Embora usualmente associada aos meios digitais, a segurança não se restringe às informações eletrônicas, aplicando-se a todos os aspectos de proteção de informações e dados, inclusive em meios físicos e verbais.

Esta Política aplica-se a todos os sócios, colaboradores e prestadores de serviços com vínculo com a Gestora, e observa a Resolução CVM nº 21/2021, o Código ANBIMA de Regulação e Melhores Práticas para a Administração de Recursos de Terceiros e suas regras de segurança cibernética, bem como a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Em atendimento ao Código ANBIMA de Administração de Recursos de Terceiros, a LAPB declara manter, em sua sede, documento contendo regras, procedimentos e controles de segurança cibernética que contempla:

I. avaliação de riscos, com identificação dos ativos relevantes — equipamentos, sistemas, dados ou processos — suas vulnerabilidades e possíveis cenários de ameaças;
II. ações de proteção e prevenção destinadas a mitigar os riscos identificados;
III. descrição dos mecanismos de supervisão para cada risco identificado, de forma a verificar sua efetividade e identificar eventuais incidentes;
IV. plano de resposta a incidentes, considerando os cenários de ameaças previstos na avaliação de riscos, que permita a continuidade dos negócios ou a recuperação adequada nos casos mais graves; e
V. indicação de responsável, dentro da instituição, para tratar e responder às questões de segurança cibernética.

2. OBJETIVO

Esta Política tem como objetivo estabelecer as diretrizes de segurança da informação da LAPB, promover a implantação de regras, procedimentos e controles para o tratamento adequado das informações e a manutenção do compromisso com a proteção de informações e a segurança cibernética, bem como orientar seus colaboradores e entidades relacionadas.

3. PROGRAMA DE SEGURANÇA DA INFORMAÇÃO

3.1 Conceitos

Informação é o conjunto de dados, processados ou não, que podem ser utilizados para a produção e a transmissão de conhecimento, contidos em qualquer meio ou formato. As informações são usualmente armazenadas em meios digitais (servidores de arquivos, bancos de dados, sistemas, e-mails, aplicativos de mensagens) ou físicos (documentos, contratos e

relatórios impressos), ou ainda em forma verbal. Toda informação em posse da LAPB, produzida ou recebida, é conteúdo de valor próprio ou de terceiros, sob responsabilidade da Gestora. A segurança da informação visa proteger todos os dados em posse da Gestora contra ameaças, empregando um conjunto de regras, procedimentos e controles.

3.2 Princípios

Para a plena realização de suas atividades, a LAPB, seus colaboradores e terceiros devem observar os três princípios da segurança da informação:

- Disponibilidade: o acesso aos dados e sistemas de informação sempre que necessário, nos casos autorizados;
- Confidencialidade: o acesso às informações restritas somente por pessoas autenticadas e especificamente autorizadas;
- Integridade: a proteção do conteúdo da informação contra alterações indevidas, intencionais ou acidentais.

3.2.1 Disponibilidade

Para garantir a disponibilidade, a LAPB mantém infraestrutura robusta de hardware — servidores, equipamentos de rede, firewalls, nobreaks e links de internet — com as devidas atualizações e manutenções preventivas. Para mitigar eventual indisponibilidade por falha de equipamentos, a LAPB trabalha com provedores de internet, com sincronização “quente” do servidor de arquivos e defasagem máxima de 1 hora para o banco de dados. A LAPB realiza backups diários do servidor de arquivos e backups horários do banco de dados, armazenados em nuvem.

3.2.2 Confidencialidade

Para garantir a confidencialidade, as informações são classificadas por departamento e armazenadas de forma estruturada em locais distintos, com acessos restritos conforme o perfil de cada usuário. Os sistemas e a infraestrutura de rede da LAPB podem ser acessados somente por usuários autenticados, com login disponibilizado pela área de TI e acesso apenas aos recursos autorizados pelo Diretor de Compliance. Havendo dúvida sobre o caráter confidencial de alguma informação, deve-se consultar previamente o Diretor de Compliance.

3.2.3 Integridade

Para garantir a integridade, além de restringir o acesso a usuários autenticados e autorizados, a infraestrutura mantém agentes de proteção contra invasão — firewalls e ferramentas antivírus — nos servidores e estações de trabalho. As ferramentas contratadas pela LAPB possuem monitoramento contra invasão externa e anomalias no tráfego de dados. Todo acesso ou modificação de arquivos é registrado e monitorado em tempo real por ferramenta específica, que envia alertas em casos suspeitos, podendo bloquear o acesso automaticamente.

3.3 Responsabilidades

Departamento de TI:

- manter infraestrutura de TI que suporte os princípios de disponibilidade, confidencialidade e integridade;
- disponibilizar recursos, equipamentos e softwares adequados à função do colaborador;
- disponibilizar login de rede e endereço de e-mail apenas com acessos necessários e autorizados;
- disponibilizar acesso seguro por VPN ao ambiente interno da LAPB aos colaboradores autorizados;
- manter recursos e softwares especializados de segurança (firewall, antivírus, anti-spam), em linha com as melhores práticas;
- manter ferramentas de monitoramento com registro de acessos à rede e gravação de voz dos ramais para fins de auditoria; e
- manter ferramentas de backup operacionais em locais físicos e lógicos separados da origem.

A infraestrutura da LAPB conta com o suporte de dois prestadores especializados de TI: a Strati Soluções e Serviços em TI Ltda., responsável pela gestão e monitoramento dos ambientes de TI da LAPB; e a Nuvme Ltda., responsável pela gestão e monitoramento do ambiente na Amazon AWS, incluindo servidor de arquivos, banco de dados, hospedagem do site e backups criptografados em nuvem. A contratação de empresas especializadas agrega conhecimento e experiência na detecção, na resposta e no monitoramento contínuo de ameaças.

Departamento de Compliance:

- assegurar que a infraestrutura de TI possua os controles de segurança da informação necessários, em conformidade com a legislação vigente;
- autorizar o uso de equipamentos e o acesso a recursos de rede, e-mail, banco de dados e demais sistemas, conforme as funções dos colaboradores;
- avaliar ocorrências, suspeitas ou denúncias de comportamento divergente do programa de segurança e adotar medidas de mitigação;
- em casos de incidente ou vazamento de informações confidenciais, ainda que involuntário, comunicar o incidente internamente, prestar as primeiras orientações e convocar o Comitê Executivo para avaliar impactos e ações de redução de danos e de prevenção de recorrência;
- quando o incidente de segurança envolver dados pessoais e puder acarretar risco ou dano relevante aos titulares, providenciar a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, nos termos do art. 48 da LGPD; e
- garantir o cumprimento de todas as normas a que a LAPB esteja sujeita, a exemplo da LGPD.

Colaboradores e terceiros:

- tratar toda informação em posse da LAPB em conformidade com este programa e com as atribuições de suas funções, sujeitando-se a penalidades em caso de uso indevido;

- utilizar os equipamentos de propriedade da LAPB (desktops, notebooks ou celulares) apenas para atividades de interesse da Gestora;
- alterar imediatamente as senhas provisórias de login e e-mail, utilizar senhas fortes e ativar a autenticação em dois fatores sempre que disponível;
- solicitar ao Departamento de TI toda instalação de software ou ajuste de configuração;
- não transferir informação para meio externo (e-mail, nuvem, dispositivos portáteis ou outro armazenamento externo), salvo exceções aprovadas pelo Departamento de Compliance; e
- submeter à aprovação do Departamento de Compliance o uso de recursos pessoais para atividades profissionais, mantendo, se aprovado, sistema operacional e ferramentas de segurança originais e atualizados.

4. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O Plano de Continuidade de Negócios define as estratégias adotadas para manter o pleno funcionamento das operações em casos de adversidades, internas ou externas, que possam causar a indisponibilidade do ambiente ou de recursos necessários à operação.

A Strati é responsável pelo monitoramento da disponibilidade e pelas manutenções periódicas do hardware do ambiente, enquanto a Nuvme é responsável pela disponibilidade dos serviços replicados na nuvem (Amazon AWS).

5. DISCIPLINAS DE SEGURANÇA

O acesso, como administrador, aos sistemas de gerenciamento de informações e às plataformas em nuvem ou que possuam serviços críticos à infraestrutura interna é restrito aos administradores ou ao Departamento de TI da LAPB. Exceções devem ser previamente autorizadas.

5.1 Criptografia

Com o objetivo de garantir a segurança da informação armazenada ou transmitida, a LAPB adota técnicas de criptografia, aplicadas tanto à transmissão e ao recebimento de dados quanto aos backups, assegurando confidencialidade, autenticidade e segurança dos dados.

5.2 Credenciais e Recomendações

- as senhas são secretas, pessoais e intransferíveis, sendo proibido o compartilhamento com terceiros, e devem ser alteradas em periodicidade estabelecida internamente com base em fatores de risco;
- é necessário o bloqueio da estação ao ausentar-se e a configuração de bloqueio automático de tela após inatividade;
- é proibido o armazenamento de credenciais ou informações confidenciais em locais visíveis a terceiros, devendo a estação de trabalho ser mantida organizada;
- materiais físicos ou eletrônicos confidenciais devem ser descartados de forma a inviabilizar o acesso por terceiros;

- em caso de possibilidade de acesso indevido ou de divulgação de informação sensível, deve-se comunicar imediatamente o Diretor de Riscos e Compliance e a área de TI; e
- no desligamento de colaborador ou parceiro, o acesso ao ambiente da LAPB é imediatamente revogado.

5.3 Segurança Física do Ambiente

Os equipamentos e as instalações de processamento de informações críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

6. REVISÃO E ATUALIZAÇÃO

Esta Política deverá ser revisada e aprovada pelo Diretor de Compliance e pelo Comitê Executivo, no mínimo, a cada 24 (vinte e quatro) meses, podendo ser revisada em prazo inferior para abranger novos processos, endereçar novos riscos, atender a alterações legais ou regulatórias, ou reforçar o compromisso da Gestora com as melhores práticas de segurança da informação. Caberá ao Diretor de Compliance a atualização desta Política e a verificação de seu cumprimento, cujo resultado será incluído no Relatório Anual de Compliance.

7. TERMO DE CIÊNCIA

O Diretor de Riscos e Compliance pode ter acesso a dados sigilosos ou protegidos por lei, devendo acessá-los de forma diligente, sigilosa, com finalidade válida e pelo prazo estritamente necessário à conclusão da diligência. O Diretor de Riscos e Compliance zela para que todos os colaboradores leiam, compreendam e concordem em seguir os procedimentos aqui descritos, mediante termo de ciência arquivado pela Gestora.