Política de Segurança da Informação e Segurança Cibernética
LAPB Gestão de Recursos Financeiros LTDA

Versão 08.2022

LAPB
GESTÃO DE RECURSOS

ÍNDICE

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 de informações em posse da gestora.

Segurança da Informação está relacionada com a proteção de um conjunto de dados no sentido de preservar o valor que possuem para um indivíduo ou organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, abordados neste documento. Apesar de usualmente abordada nos meios digitais, a segurança não é restrita somente a informações eletrônicas, sistemas de armazenamento ou documentação impressa disponível, aplicando-se a todos os aspectos de proteção de informações e dados.

Esta política é aplicável a todos os colaboradores da LAPB, sócios ou funcionários, bem como a todos os prestadores de serviços que possuem vínculo com a gestora.

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

I. Avaliação de riscos, que deve identificar os ativos relevantes, sejam eles equipamentos, sistemas, dados ou processos, suas vulnerabilidades e possíveis
cenários de ameaças;
II. Ações de proteção e prevenção, visando 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. Criação de um plano de resposta a incidentes, considerando os cenários de ameaças
previstos durante a avaliação de riscos, que permita a continuidade dos negócios ou
a recuperação adequada em casos mais graves; e
V. Indicação de responsável dentro da instituição para tratar e responder questões de
segurança cibernética.

2. OBJETIVO

A 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 manutenção do compromisso com a proteção de informações e segurança cibernética (cibersegurança), bem como orientar seus colaboradores e entidades relacionadas à gestora.

3. PROGRAMA DE SEGURANÇA DE INFORMAÇÃO

3.1 CONCEITOS

O **conceito de informação** pode ser definido como: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio ou formato.

As **informações são usualmente armazenadas** em meios digitais, como servidores de arquivos, banco de dados, sistemas de informação, e-mails, aplicativos de mensagens ou pen-drive, ou em meios físicos, como documentos, contratos e relatórios impressos, ou em forma oral como uma conversa em espaço público.

Toda **informação em posse da LAPB**, produzidas ou recebidas, são conteúdos de valor próprio ou de valor para terceiros que estão sob responsabilidade da gestora.

A **segurança da informação** visa proteger todos dados em posse da gestora contra perigos e ameaças, empregando um conjunto de regras, procedimentos e controles que minimizam a ocorrência de eventos e danos indesejáveis.

3.2 PRINCÍPIOS

Para a plena realização de suas atividades, a LAPB, seus colaboradores e terceiros devem seguir os 3 princípios de segurança da informação que visam garantir:

- *Disponibilidade*: o acesso aos dados e sistemas de informação sempre que for necessário em casos autorizados;

- *Confidencialidade*: o acesso às informações restritas somente pelas pessoas autenticadas e especificamente autorizadas;

- *Integridade*: a proteção do conteúdo da informação contra alterações indevidas, sejam elas intencionais ou acidentais.

3.2.1 DISPONIBILIDADE

Para garantir **disponibilidade**, a LAPB deve manter uma infraestrutura robusta de hardwares como servidores, equipamentos de rede, firewalls, nobreaks e links de internet com as devidas atualizações e manutenções preventivas.

De forma a mitigar eventual indisponibilidade por falhas de equipamentos, a LAPB trabalha com um ambiente redundante de contingência e provedores de internet com sincronização "quente" do

servidor de arquivos e defasagem máxima de 1 hora para o banco de dados.

Ainda, caso seja necessário, a LAPB realiza backups diários do servidor de arquivos e backups de hora em hora do banco de dados em armazenamento na nuvem.

3.2.2 CONFIDENCIALIDADE

Para garantir **confidencialidade**, as informações são classificadas por departamento e armazenadas de forma estruturada em locais distintos com acessos restritos de acordo com o perfil de cada usuário.

Os sistemas e infraestrutura de rede da LAPB podem ser acessadas somente por usuários autenticados com login disponibilizado pela área de TI e com acesso somente aos recursos autorizados pelo Diretor de *Compliance*.

Na ocorrência de qualquer tipo de dúvida sobre o caráter confidencial de alguma informação, deve-se consultar previamente o Diretor de *Compliance* para obtenção de orientação adequada.

3.2.3 INTEGRIDADE

Para garantir **integridade**, além das informações, recursos e sistemas estarem acessíveis apenas a usuários autenticados e autorizados, a infraestrutura deve manter agentes de proteção contra invasão como firewalls e ferramentas antivírus nos servidores e estações de trabalho dos usuários.

As ferramentas contratas pela LAPB possuem monitoramento contra invasão externa e anomalias no tráfego de dados. Em complemento, todo acesso ou modificação de arquivos são registrados e monitorados em tempo real por ferramenta específica que envia alertas em casos suspeitos, podendo inclusive bloquear acesso de forma automática.

3.3 O PROGRAMA

O **programa de segurança de informação** da LAPB relaciona um conjunto de medidas que visam a proteção das informações, bem como orientações de uso adequado dos colaboradores e terceiros para apoiar e suportar as atividades da gestora.

Para um programa robusto é preciso que todos envolvidos façam sua parte, agindo sempre com zelo no trato e no envio de informações que extrapolam o domínio da LAPB.

Para melhor organização das atribuições e responsabilidades, a seguir temos as principais ações e responsabilidades que devem ser seguidas, segregadas por função abaixo:

3.3.1 RESPONSABILIDADES DO DEPARTAMENTO DE TI

O departamento de TI deve manter uma infraestrutura de TI que suporte da melhor forma possível os princípios de disponibilidade, confidencialidade e integridade.

Disponibilizar recursos, equipamentos e softwares adequados para a função do colaborador.

Disponibilizar login de rede e endereço de e-mail somente com acessos a recursos necessários e autorizados à função do colaborador.

Disponibilizar acesso seguro VPN ao ambiente interno da LAPB aos colaboradores autorizados.

Manter recursos e softwares especializados de segurança para a proteção da infraestrutura contra ameaças (*firewall*, anti-vírus, *anti-spam*), em linha com a melhores práticas de segurança.

Manter ferramentas de monitoramento com registro de acessos à rede e gravação de voz dos ramais para fins de auditoria.

Manter ferramentas de backup operacionais em locais físicos e lógicos separados do local de origem.

A infraestrutura da LAPB conta com o suporte e assessoria de dois provedores de serviços de TI, a Strati Soluções e Serviços em TI Ltda. (www.strati.com.br) e a Nuvme Ltda. (www.nuvme.com.br):

- **STRATI SOLUCOES E SERVICOS EM TI LTDA**: empresa responsável pela gestão e monitoramento dos ambientes de TI da LAPB, incluindo o escritório localizado no Itaim Bibi e o ambiente de contingência no Morumbi;

- **NUVME LTDA**: empresa responsável pela gestão e monitoramento do ambiente da LAPB na Amazon AWS, incluindo o servidor de arquivos, banco de dados, hospedagem do site da LAPB e backups criptografados em nuvem.

A adoção de empresas especializadas de TI agrega maior conhecimento e experiência tanto na detecção quanto na implementação de respostas e monitoramento contínuo das ameaças.

3.3.2 RESPONSABILIDADES DO DEPARTAMENTO DE COMPLIANCE

O departamento de *Compliance* deve assegurar que a infraestrutura de TI da LAPB possua os controles de segurança de informação necessários em conformidade com a legislação vigente.

Autorizar o uso de equipamentos, acesso a recursos de rede, e-mail, banco de dados e outros sistemas em conformidade com as funções dos colaboradores.

Avaliar ocorrências, suspeitas ou denúncias de comportamento divergente ao programa de segurança de informação, bem como trabalhar na adoção de medidas que possam contribuir na mitigação do problema.

Em casos de vazamento de informações confidenciais, mesmo que oriundos de ações involuntárias, comunicar incidente aos colaboradores e dar primeiras orientações quanto a questionamentos externos. Em seguida, organizar um Comitê Executivo para avaliar impactos e ações para redução de danos, além de avaliação de medidas adicionais necessárias para mitigar a possibilidade de recorrência de impactos similares.

Garantir o estrito cumprimento de todas as normas que a LAPB esteja sujeita, a exemplo da Lei Geral de Proteção de Dados (LGPD).

3.3.3 RESPONSABILIDADES DOS COLABORADORES DA LAPB E TERCEIROS

Toda informação em posse da LAPB disponível aos colaboradores e terceiros deve ser tratada em conformidade com as regras deste programa e atribuições de suas funções. O uso indevido ou inadequado das informações estará sujeito a análise e penalidades podem ser aplicadas.

Todo equipamento de uso individual (desktops, notebooks ou celulares) de propriedade da LAPB são recursos disponibilizados para a realização das atividades de interesse da gestora.

Todo colaborador recebe um login de rede próprio e um endereço de e-mail com senhas provisórias que devem ser imediatamente alteradas. Em sistemas de terceiros, a recomendação é cadastrar login único por usuário sempre que for possível.

Em todos os casos, os usuários devem utilizar senhas "fortes" e ativar a autenticação em 2 fatores sempre que estiver disponível.

O usuário é corresponsável pela proteção da integridade do equipamento, toda instalação de software ou ajuste de configuração devem ser solicitadas ao departamento de TI.

É proibida a transferência de informação para uso em meio externo, seja por e-mail, armazenamento em nuvem, dispositivos portáteis ou qualquer outro sistema de armazenamento externo à infraestrutura da LAPB, salvo exceções aprovadas pelo departamento de *Compliance*.

O uso de recursos pessoais (*desktops*, *notebooks* ou celulares) para realização de atividades profissionais deve ser submetido à aprovação pelo departamento de *Compliance*. Em caso de aprovação, é mandatório que o recurso pessoal mantenha sistema operacional com as devidas ferramentas de segurança e softwares originais sempre atualizados.

4. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

Também conhecido como plano de continuidade operacional, o PCN define as estratégias adotadas para manter o pleno funcionamento das operações em casos de adversidades causadas por fatores internos ou externos à gestora e que possam causar a indisponibilidade do ambiente ou quaisquer recursos necessários na operação.

A LAPB possui posições de trabalho estratégicas contratadas no bairro do Morumbi em parceria com a empresa Regus do Brasil LTDA. A empresa é responsável pelo espaço físico, garantia de disponibilidade de acesso à internet, controle de acesso físico e limpeza ao ambiente.

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

O site de contingência é monitorado de forma remota pela empresa Strati, com atualizações dos softwares sendo periodicamente realizadas. Além do acesso remoto que possuímos ao ambiente, testes presenciais são realizados periodicamente para avaliar a integridade dos sistemas.

5. DISCIPLINAS DE SEGURANÇA

O acesso como administrador aos sistemas de gerenciamento de informações e plataforma em nuvem ou que possuam serviços críticos à infraestrutura interna são restritos aos administradores ou ao TI da LAPB. Exceções devem ser autorizadas previamente.

5.1. CRIPTOGRAFIA

Com o objetivo de garantir a segurança da informação armazenada ou transmitida, a LAPB adota técnicas de criptografia. Os recursos são utilizados no sentido de assegurar a confidencialidade, autenticidade e segurança de dados, seguindo as regras de segurança de informação e padrões de segurança.

A criptografia é aplicada tanto para transmissão e recebimento de dados, assim como utilizada nos backups de dados.

5.2. CREDENCIAIS E RECOMENDAÇÕES

- A senhas são secretas, pessoais e intransferíveis, sendo expressamente proibido o compartilhamento de senhas com terceiros. Em periodicidade estabelecida internamente com base em fatores de risco, as senhas devem ser alteradas;
- Para garantia de segurança de acesso local aos computadores, é necessário o bloqueio da estação ao ausentar-se da máquina e a configuração do bloqueio automático de tela após inatividade;

- É proibido o armazenamento de credenciais (senhas) ou informações confidenciais em locais que possam ser visualizados por terceiros, sendo necessário manter a estação de trabalho organizada;
- Materiais físicos ou eletrônicos confidenciais/sensíveis devem ser descartados adequadamente para inviabilizar acessos por terceiros;
- Em caso de possibilidade de acesso indevido ou divulgação de qualquer tipo de informação sensível, deve-se imediatamente realizar a comunicação ao Diretor de Risco e TI e Diretor de *Compliance*;
- No caso de desligamento de funcionário ou parceiro, é imediatamente revogado o acesso ao ambiente da LAPB.

5.3. SEGURANÇA FÍSICA DO AMBIENTE

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

O espaço de contingência no Morumbi também possui acesso restrito e limitado às pessoas autorizadas pela LAPB.

6. REVISÃO E ATUALIZAÇÃO

Esta Política poderá ser revisada ou atualizada a qualquer momento para abranger novos processos, identificar novos riscos ou reforçar o compromisso da gestora com as melhores práticas de segurança da informação.

7. TERMO DE CIÊNCIA

Os Diretores de Risco e Compliance podem ter acesso a dados sigilosos ou protegidos por lei, sempre deverão acessar estes dados de forma diligente, sigilosa, com finalidade válida e em prazo máximo até que a diligência seja concluída.

Os Diretores de Risco e Compliance atestam que todos os colaboradores leram, entenderam e concordaram em seguir os procedimentos aqui descritos.