1. OBJETIVO

Esta Política de Segurança Cibernética aplica-se a Lastro RDV DTVM LTDA., e a todos os seus administradores, colaboradores e terceiros e tem como objetivo definir e garantir a aplicação dos princípios, diretrizes e das ações necessárias para assegurar a confidencialidade, integridade e a disponibilidade dos dados e dos sistemas de informação, de forma a prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, em conformidade com a Resolução CMN nº 4.893/2021.

1.2 CONCEITOS E DEFINIÇÕES

Administradores – Todos os membros do conselho de administração, diretoria e comitês, estatutários ou não, da LASTRO.

Colaboradores - Todos os funcionários, menores aprendizes e estagiários da LASTRO.

CyberSecurity - É o termo que designa o conjunto de controles e tecnologias que visam proteger de danos e intrusão ilícita, programas, computadores, redes e dados.

Phishing - Uma técnica utilizada por criminosos digitais usam para enganar as pessoas a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Tal técnica é praticada costumeiramente por envio de e-mails falsos e/ou do redirecionamento a websites falsos.

2. Diretrizes

A Segurança da Informação estabelece os principais controles e diretrizes, conforme a seguir indicados:

As informações da LASTRO devem ser tratadas de forma ética e sigilosa respeitando-se os princípios da privacidade, bem como as leis aplicáveis em vigor, evitando o mau uso das informações e a exposição indevida da Lastro.

As informações da LASTRO devem ser utilizadas de forma transparente e exclusivamente para a finalidade em que foi autorizada a coleta ou tratamento dos dados.

Todo o processo durante o ciclo de vida da informação deve garantir a segregação de funções para garantir que a atividade não seja executada e controlada pelo mesmo colaborador e/ou equipe, de modo a promover maior segurança das informações da Lastro.

A identificação ou acesso (login e senha) aos ambientes tecnológicos de sistemas de qualquer colaborador deve ser único, pessoal e intransferível, de modo a possibilitar a

identificação daquele que desempenhou determinada atividade. O compartilhamento de acessos é terminantemente proibido, ficando o colaborador sujeito a toda e qualquer responsabilidade decorrente da violação das diretrizes e procedimentos aqui estabelecidos.

A concessão de acessos deve obedecer ao critério de menor privilégio, ou seja, conceder o mínimo de acesso, de forma imprescindível para desempenho de suas atividades.

As informações devem ser classificadas levando em consideração a sua relevância, requisitos legais, sensibilidade e criticidade, evitando assim sua modificação, divulgação ou descarte não autorizado. Todos os Colaboradores devem seguir as melhores práticas recomendadas no Manual de Boas Práticas do uso da Tecnologia da Informação disponibilizado pela LASTRO.

O colaborador deve:

• Manter a confidencialidade da senha, devendo memorizá-la e ao invés de registrá-la ou anotá-la em lugar algum;

• Abster-se de revelar a senha a terceiros;

• Adotar sempre que disponível o fator duplo de autenticação;

• Alterar a senha sempre que existir qualquer suspeita de seu comprometimento ou sempre que expirar;

• Selecionar senhas fortes e de difícil adivinhação;

• Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/logado com a sua identificação;

• Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del);

• Nunca utilizar o e-mail corporativo para fins pessoais tais como redes sociais ou acessos não autorizados pela LASTRO;

• Realizar todos os treinamentos relativos ao fortalecimento da conscientização da cultura de segurança da informação e prevenção contra ameaças de Phishing;

• Nunca adotar ferramentas, aplicativos, sistemas entre outros para compartilhamento de informações da LASTRO que não estejam homologadas previamente pelas áreas de tecnologia, segurança e jurídica.

• Nunca compartilhar informações da LASTRO em mídias sociais, aplicativos de mensagens entre outros sem previa autorização, como por exemplo, Facebook, Whatsapp, Linkedin, etc.

2.1 Conscientização em Segurança Cibernética

A LASTRO promove a disseminação dos princípios e diretrizes de segurança cibernética por meio de:

(i) divulgação de informações a usuários sobre as precauções na utilização de produtos e serviços financeiros; e

(ii) ações de comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

Todos os colaboradores devem realizar o treinamento “Boas Práticas para a Segurança da Informação”, disponibilizado pela LASTRO.

2.2. Governança com as áreas de negócio e tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhados com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações bem como uma arquitetura segura de modo a evitar indisponibilidade dos ambientes

2.3. Princípios

O compromisso da LASTRO com o tratamento adequado das informações está fundamentado nos seguintes princípios:

Confidencialidade: garantia de que as informações tratadas sejam de conhecimento exclusivo das pessoas especificamente autorizadas;

Integridade: garantia de que as informações sejam mantidas íntegras, sem modificações indevidas, sejam elas acidentais ou propositais; e

Disponibilidade: garantia de que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

As informações podem estar presentes em diversos meios, tais como, mas não se limitando a, sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, nuvem e até mesmo por meio da comunicação oral.

Todas as informações recebidas pelos colaboradores e administradores da LASTRO que sejam acessadas, armazenadas, geradas ou desenvolvidas nas dependências ou de terceiros contratados, durante a execução das suas atividades, são de titularidade da LASTRO, não

podendo ser estendidas, seja a que título for, como transferência de titularidade ou de direito de propriedade intelectual.

A área de Segurança da Informação deverá ser envolvida em toda aquisição, desenvolvimento ou manutenção de um sistema/aplicação ou serviços tecnológicos na LASTRO, para que possa avaliar ou recomendar os requisitos mínimos de segurança, assim mitigando ou minimizando os impactos ao negócio.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas ou oriundas de erros, fraudes, vandalismo, espionagem, sabotagem ou qualquer outro motivo, estarão sujeitas às penalidades previstas nos contratos celebrados com a LASTRO, sem prejuízo das perdas e danos decorrentes.

3. GESTÃO DE SEGURANÇA CIBERNÉTICA E INFORMAÇÃO

A LASTRO possui políticas e procedimentos para assegurar que as informações estejam adequadamente protegidas, baseadas nos requerimentos mínimos exigidos pelos Órgãos Reguladores, nas melhores práticas reconhecidas pelo mercado, sendo estabelecidas as seguintes diretrizes:

Gestão de Ativos da Informação, Acesso e Controle de Acesso: os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, de eventuais adulterações de dados e ter documentação e planos de manutenção atualizados; as concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transação;

Classificação da Informação: as informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, e de acordo com a classificação dos níveis de relevância. Adotamos quatro categorias para efeitos de classificação de informações:

- Público;
- Interno;
- Confidencial;
- Estratégico;

Gestão de Acessos: as concessões, revisões e exclusões devem basear-se em conceitos de autoridade, autenticidade e privilégios mínimos de acesso. Os acessos devem ser rastreáveis, a fim de garantir a identificação de acesso e transação;

Garantia da Continuidade de Negócios: O gerenciamento de riscos deve garantir a manutenção da continuidade dos negócios, abrangendo serviços relevantes e a capacidade de continuar a entrega de produtos ou serviços em um nível mínimo aceitável e previamente definido, quando da ocorrência de um evento que interrompa as operações;

Conscientização sobre segurança cibernética: a LASTRO deve garantir a disseminação dos princípios e diretrizes de Segurança cibernética, fortalecendo a cultura de segurança cibernética e informação, em todos os níveis operacionais.

Riscos Cibernéticos: utilização de firewall nos links e softwares de antivírus nas estações e servidores, para diminuir os riscos de ataques cibernéticos, internos ou externos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDos e Botnets), sabotagem, bem como violação de acessos e privacidade, que podem desproteger os dados, redes e sistemas da empresa causando danos financeiros e de reputação ou imagem.

4. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A LASTRO, quando da utilização de serviços em nuvem, atenderá aos critérios previstos na Resolução nº 4.893/2021 do CMN, considerando a avaliação de risco que estes representam para o negócio.

5. CRITÉRIOS PARA DECISÃO SOBRE TERCEIRIZAÇÃO DE SERVIÇOS

Para garantir conformidade com o Art. 11º da Resolução CMN nº 4.893/21, a Lastro RDV DTVM LTDA. estabelece os seguintes critérios para decisão sobre a terceirização de serviços relacionados à segurança cibernética:

Avaliação de Risco: Qualquer contratação de prestadores de serviço deverá ser precedida de uma avaliação de risco, incluindo análise de vulnerabilidades e impacto potencial no ambiente cibernético da instituição.

Requisitos de Segurança: Os fornecedores devem atender a requisitos mínimos de segurança, incluindo conformidade com normas, bem como aderência às boas práticas do mercado financeiro.

Contrato e SLAs: Todos os contratos firmados com terceiros devem conter cláusulas específicas que garantam a segurança da informação, níveis mínimos de serviço (SLAs) e mecanismos de auditoria e monitoramento contínuos.

Monitoramento Contínuo: A Lastro realizará monitoramento contínuo dos prestadores de serviço terceirizados para garantir conformidade com as diretrizes internas e regulatórias.

Plano de Contingência: Todos os fornecedores devem apresentar um plano de resposta a incidentes e continuidade de negócios, assegurando a rápida recuperação de serviços em caso de falha ou ataque cibernético.

Rescisão e Descontinuidade: A instituição estabelecerá diretrizes para a descontinuação de serviços terceirizados, garantindo a revogação segura de acessos e a destruição ou devolução segura de dados sensíveis.

Esta seção reforça o compromisso da Lastro com a gestão segura de prestadores de serviço e assegura a conformidade com a regulamentação vigente.

6. RESPONSABILIDADE E COMUNICAÇÃO

O cumprimento da Política de Segurança Cibernética da LASTRO 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 LASTRO, 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 o departamento de Compliance, pelo e-mail disponibilizado: compliance@lastro.com.br

7. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÕES

Esta política tem vigência de 1 (um) ano e deve ser revisada anualmente ou em prazo inferior, se houver alguma alteração nas leis e regulamentos aplicáveis ou alteração das práticas da LASTRO RDV DTVM LTDA, que justifiquem a atualização desta política.

EVENTO	DATA DE APROVAÇÃO	DIRETORIA
Implementação	27/06/2017	DIRETORIA EXECUTIVA
1ª revisão	29/03/2023	DIRETORIA EXECUTIVA
2ª revisão	27/06/2023	DIRETORIA EXECUTIVA
3ª revisão	30/04/2024	DIRETORIA EXECUTIVA
4ª revisão	18/03/2025	DIRETORIA EXECUTIVA