I. OBJETIVO

A Lastro tem por objetivo estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação cibernética e promover a melhoria continua 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 da empresa.

II. PRINCIPAIS CONCEITOS

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos, incluindo os controles relacionados aos serviços de nuvem contratados.

Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

Integridade: salvaguarda da exatidão e dos métodos de processamento da informação.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

III. 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:
Adota quatro categorias para efeitos de classificação da informação:

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.

IV. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A Lastro, quando da utilização de serviços em nuvem, atenderá aos critérios previstos na Resolução 4.658/2018 do CMN, considerando a avaliação de risco que estes representam para o negócio.

V. 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 alta Administração da 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