1. OBJETIVO

Estabelecer as diretrizes e responsabilidades para garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações da Larca Capital, protegendo seus ativos tecnológicos e dados pessoais contra acessos não autorizados, vazamentos, incidentes cibernéticos e demais ameaças internas ou externas.

2. ABRANGÊCIA

Esta Política de Segurança da Informação aplica-se às empresas do Grupo Larca Capital (Larca Capital Fundo de Investimento em Direitos Creditórios, Larca Capital Securitizadora S.A., Larca Promotora de Vendas Ltda., MC Cobrança e Análise de Crédito Ltda., Lar Cobrança e Análise de Crédito Ltda. e Larca Capital – Sociedade de Crédito Direto S.A.) que processem ou acessem dados pessoais ou corporativos, observados os limites de alçada, a segregação de acessos e a estrita necessidade de tratamento para o desempenho das respectivas atividades, em conformidade com a Resolução CMN nº 4.893/2021 e demais normas aplicáveis.

Não há compartilhamento irrestrito ou unificação de bancos de dados entre as empresas do grupo, sendo todo e qualquer acesso ou tratamento realizado com base em controles de segurança, confidencialidade e finalidade legítima, conforme as diretrizes desta Política.

3. REFERÊNCIAS NORMATIVAS

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD);
- Resolução CMN nº 4.893/2021 – Estrutura de Governança, Riscos e Controles Internos;
- ISO/IEC 27001 e 27002 – Sistema de Gestão de Segurança da Informação (SGSI);
- Normas e Procedimentos Larca Capital NP-106-Procedimento de Gestão de SI em Fornecedores e Nuvens de Dados a NP-107-Gestão de Riscos e Avaliações de Impacto em Proteção de Dados.

4. PRINCÍPIOS

- Confidencialidade: acesso restrito às pessoas autorizadas;
- Integridade: proteção contra alterações não autorizadas;
- Disponibilidade: acesso contínuo às informações e serviços essenciais;
- Autenticidade e Não Repúdio: garantia de que usuários e sistemas são legítimos;
- Responsabilização: manutenção de evidências e rastreabilidade de ações.

5. DIRETRIZES GERAIS

- Toda informação tratada pela Larca Capital é de propriedade da instituição;
- O uso de e-mail, internet e dispositivos corporativos é exclusivo para fins profissionais;
- É proibido o compartilhamento não autorizado de informações corporativas;
- Todas as comunicações de incidentes devem seguir o NP-104 – Procedimento de Resposta a Incidentes;

- Fornecedores e prestadores de serviço devem cumprir os requisitos definidos no NP-106 – Gestão de Segurança da Informação em Fornecedores e Nuvens;
- Todos os colaboradores devem cumprir a norma NP-102-Procedimento de Endpoints, garantindo dispositivos criptografados e monitorados.

6. GESTÃO DE RISCOS E CONTINUIDADE

A Larca Capital mantém um processo formal de gestão de riscos cibernéticos e de continuidade, conforme:

- NP-105 – Plano de Continuidade de Negócios e TIC: define as ações para garantir a operação durante incidentes ou desastres;
- NP-107 – Gestão de Riscos e Avaliação de Impacto em Proteção de Dados (RIPD/DPIA): identifica e mitiga riscos em tratamentos de dados pessoais;
- Revisões anuais e testes simulados de contingência supervisionados pelo Comitê de Segurança e pelo CISO.

7. CONTROLE DE ACESSO

- O acesso aos sistemas corporativos é individual, controlado e autenticado por credenciais pessoais (login e senha), devendo, sempre que disponível, ser complementado por autenticação multifator (2FA), garantindo maior segurança e rastreabilidade das ações do usuário.
- Perfis de acesso seguem o modelo RBAC (Role Based Access Control), conforme definido em NP-108 – Acesso Privilegiado;
- Todo acesso remoto deve ser realizado exclusivamente por meio de VPN corporativa criptografada (IPSEC-VPN), assegurando a confidencialidade, integridade, autenticação e rastreabilidade das conexões.
- Contas inativas ou de ex-colaboradores são bloqueadas imediatamente após o desligamento.

8. GESTÃO DE LOGS E MONITORAMENTO

- Todos os eventos relevantes são registrados e auditáveis conforme NP-109 – Gestão e Retenção de Logs;
- Os logs devem ser armazenados de forma segura, em ambiente controlado, com mecanismos que assegurem sua integridade, autenticidade e rastreabilidade, como controle de acesso restrito, trilhas de auditoria e armazenamento imutável.
- O ambiente é monitorado 24x7 via SIEM, com alertas automáticos para tentativas de acesso indevido ou anomalias.

9. DESENVOLVIMENTO SEGURO

Conforme NP-110 – Desenvolvimento Seguro, todo software, sistema ou integração contratado de terceiros deverá atender às recomendações mínimas de segurança previstas na Resolução CMN nº 4.893/2021, garantindo conformidade com os controles internos da Larca Capital.

10. CONTROLE DE ENDPOINTS

Os dispositivos corporativos ou pessoais que acessam sistemas da Larca Capital devem:

- Estar criptografados (BitLocker);
- Possuir antivírus ativo e atualizado;
- Bloquear automaticamente após 5 minutos de inatividade;
- Ser gerenciados via Google Endpoint Management e GLPI;
- Cumprir integralmente o NP-102 – Controle de Endpoints.

11. RESPOSTAS A INCIDENTES:

- Todo incidente deve ser comunicado imediatamente ao CISO, conforme NP-104 – Procedimento de Gestão e Respostas a Incidentes;
- A comunicação a autoridades (BACEN, ANPD, COAF ou Polícia Federal) seguirá o NP-101 – Procedimentos de Contato com Autoridades;
- Após cada incidente, é elaborado Relatório de Lições Aprendidas com recomendações de melhoria contínua.

12. TREINAMENTO E CONSCIENTIZAÇÃO

- Todos os colaboradores devem participar de treinamentos obrigatórios anuais em segurança da informação e proteção de dados;
- A política de "Mesa Limpa e Tela Limpa" é obrigatória para evitar exposição de dados sensíveis;
- Simulações e campanhas educativas são conduzidas periodicamente pelo DPO e CISO.

13. PENALIDADES E RESPOSNABILIDADES

O descumprimento das diretrizes desta política poderá resultar em:

- Suspensão de acessos;
- Advertência formal;
- Medidas disciplinares previstas no código de conduta e, quando aplicável, comunicação às autoridades competentes.

14. REVISÃO E ATUALZIAÇÃO

Esta política será revisada anualmente ou sempre que houver alterações tecnológicas, regulatórias ou organizacionais relevantes, sendo aprovada pela Diretoria Executiva e registrada em ata de reunião.

15. DISPOSIÇÕES FINAIS

Esta Política integra o Programa de Governança de Segurança da Informação e Proteção de Dados da Larca Capital e complementa a PL001-Política de Privacidade e Termo de Uso da instituição, devendo ser amplamente divulgada nos canais internos e acessível a todos os colaboradores, prestadores de serviço e parceiros comerciais.