1. OBJETIVO

Estabelecer diretrizes para proteger informações da Larca Capital, clientes, investidores, parceiros e fornecedores, reduzindo vulnerabilidades, prevenindo incidentes e assegurando a continuidade dos serviços, em alinhamento às normas regulatórias.

2. ÂMBITO DE APLICAÇÃO

Aplica-se as empresas do Grupo Larca Capital: (Larca Capital Fundo de Investimento em Direito Creditório, 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, observados os limites de alçada, 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, sem compartilhamento irrestrito ou unificação de bancos de dados entre as empresas do grupo.

3. NORMAS APLICÁVEIS

- Resolução CMN nº 4.893/2021 – Serviços de TI e Nuvem
- Resolução Conjunta CMN/BCB nº 6/2023 – Compartilhamento de Fraudes
- LGPD – Lei nº 13.709/2018
- Lei Complementar nº 105/2001 – Sigilo Bancário

4. DEFINIÇÕES

- Ativos: dados, sistemas, documentos físicos e digitais, redes e infraestruturas tecnológicas.
- Segurança da Informação: proteção contra acesso, alteração, destruição ou divulgação não autorizada.
- Segurança Cibernética: tecnologias e processos para proteção contra-ataques, fraudes e incidentes digitais.
- Log: registro de eventos de sistemas para auditoria e rastreabilidade.

5. PRINCÍPIOS FUNDAMENTAIS

Garantir a Confidencialidade, Integridade e Disponibilidade das informações da Larca Capital e de todos os envolvidos, assegurando acesso restrito apenas a pessoas autorizadas, dados íntegros e transparentes e disponibilidade garantida sempre que necessário.

6. DIRETIZES GERAIS

- Controle de Acesso, Segregação de Funções e Princípio do Menor Privilégio
- Gestão de Identidades e Credenciais de Acesso
- Prevenção a Vazamentos e Proteção das Informações
- Monitoramento Contínuo e Mecanismos Antifraude
- Gestão e Comunicação de Incidentes de Segurança

7. GESTÃO ATIVOS E CLASSIFICAÇÃO DA INFORMAÇÃO

Inventário atualizado de ativos e a seguinte classificação por criticidade:

- Informação Publica: sem restrição.
- Informação Restrita: uso apenas por áreas específicas.
- Informação Confidencial: informação sigilosa com acesso restrito autorizado.

8. AUTENTICAÇÃO, ACESSO, SEGMENTAÇÃO DE REDE

- Autenticação multifator (MFA) para sistemas críticos quando existente.
- Segregação de redes, VPN segura e proteção contra acesso externo indevido.
- Controle de tráfego limitando a comunicação entre segmentos para reduzir riscos de invasão e movimentação lateral.
- Revisão periódica de acessos e auditoria regular de permissões, desativação imediata de contas em casos de desligamento e controle contínuo para evitar acessos indevidos.

9. BACKUP, CRIPTOGRAFIA E PROTEÇÃO CONTRA MALWARE

- Rotinas de backup com testes de restauração conforme NP-103–Backup e Recuperação de Dados.
- Criptografia para dados em trânsito e em repouso.
- Sistemas de detecção e prevenção contra malware e phishing conforme NP-102-Controle de Endpoints.

10. GESTÃO DE INCIDENTES E PLANO DE RESPOSTA

- Classificação de incidentes por criticidade e impacto.
- Registro, análise e plano de mitigação para todos os incidentes.
- Comunicação imediata aos órgãos reguladores e parceiros para incidentes relevantes conforme NP-104- Procedimento Gestao e Respostas a Incidentes.

11. RELÁTORIO ANUAL DE INCIDENTES

- Data-base: 31/12 de cada ano.
- Entrega até 31/03 do ano seguinte à Alta Administração e, quando aplicável, aos órgãos reguladores.
- Conteúdo: incidentes, ações corretivas, resultados de testes de continuidade.

12. GESTÃO DE FORNECEDORES E SERVIÇOS DE NUVEM

- Contratos com cláusulas de confidencialidade, continuidade, integridade e auditoria.
- Comunicação aos órgãos reguladores para serviços relevantes e incidentes críticos.

13. SEGURANÇA FÍSICA E CONTINUIDADE DOS SERVIÇOS

- Controle de acesso a áreas restritas.
- NP-105-Plano de Continuidade de Negócios (PCN) com RTO/RPO definidos.

14. COMPARTILHAMENTO DE INFORMAÇÕES E COMUNICAÇÃO AO BACEN

- Compartilhamento de indícios de fraude conforme Res. Conjunta nº 6/2023.
- Comunicação tempestiva ao Bacen para incidentes críticos e interrupções.

15. TREINAMENTOS, CULTURA E CONSCIENTIZAÇÃO

- Programas anuais de capacitação e simulações de incidentes.
- Divulgação da política em linguagem clara a colaboradores e parceiros.

16. ARQUIVAMENTO E RETENÇÃO DOCUMENTOS

Retenção por 5 anos: política, atas, relatórios anuais, contratos e registros de incidentes.

17. DISPOSIÇOES GERAIS E REVISÃO

- Revisão anual ou sempre que houver mudanças regulatórias relevantes.
- Aprovação pela Alta Administração e disponibilização pública da versão vigente.