Política de Segurança da Informação

Julho 2026

Nome	Política Segurança da Informação
Aplicabilidade	Sócios, administradores, funcionários e todos que auxiliam nas atividades da Latache Capital.
Data de Início	01/08/2026
Revisado por Compliance em	01/08/2026
Versão	V.01

1. OBJETIVO

Estabelecer diretrizes, responsabilidades, controles e práticas mínimas de segurança da informação para proteger os ativos de informação da GESTORA contra acessos não autorizados, uso indevido, alteração, perda, indisponibilidade, divulgação indevida ou destruição, assegurando a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e conformidade legal das informações corporativas.

2. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

- **Confidencialidade:** garantir que as informações sejam acessadas somente por pessoas, processos ou sistemas devidamente autorizados.
- **Integridade:** preservar a exatidão, completude e consistência das informações durante todo o seu ciclo de vida.
- **Disponibilidade:** assegurar que as informações e serviços estejam acessíveis aos usuários autorizados sempre que necessário.
- **Rastreabilidade:** manter registros suficientes para permitir auditoria, investigação de incidentes e comprovação de conformidade.
- **Privacidade e Proteção de Dados:** tratar dados pessoais e informações sensíveis conforme a legislação aplicável e as políticas internas.

3. RESPONSABILIDADES

Colaboradores e prestadores de serviços: devem cumprir esta política, utilizar os recursos corporativos exclusivamente para fins profissionais, proteger credenciais de acesso, reportar incidentes ou suspeitas de incidentes e zelar pela segurança das informações sob sua responsabilidade.

Gestores: devem promover a conscientização de suas equipes, garantir que acessos sejam concedidos conforme necessidade de negócio, comunicar admissões, movimentações e desligamentos em tempo hábil e apoiar a aplicação das diretrizes desta política.

Compliance: deve manter esta política atualizada, avaliar riscos e conformidade, apoiar a definição de controles, acompanhar indicadores de segurança, recomendar melhorias e assegurar que as práticas estejam alinhadas aos requisitos legais, regulatórios e corporativos.

Tecnologia da Informação: deve implementar, operar e monitorar controles técnicos de segurança, administrar identidades e acessos, manter ativos tecnológicos protegidos e atualizados, tratar incidentes de segurança e preservar registros necessários para auditoria.

4. CONTROLE DE ACESSO E USO DA REDE

- Todo acesso aos recursos corporativos deve ser concedido com base no princípio do menor privilégio e na necessidade de conhecimento.
- A criação, alteração, revisão e revogação de acessos deve ocorrer mediante solicitação formal, aprovação do gestor responsável e registro em chamado.
- Contas de usuários desligados, transferidos ou com mudança de função devem ser bloqueadas ou ajustadas tempestivamente.

- O uso de autenticação multifator deve ser obrigatório para acessos remotos, aplicações em nuvem e sistemas críticos.
- Redes corporativas e redes de visitantes devem ser segregadas, com controles de autenticação, registro e restrição de acesso ao ambiente interno.

5. USO DE E-MAIL CORPORATIVO

O e-mail corporativo deve ser utilizado exclusivamente para fins profissionais e em conformidade com as políticas internas. Os usuários devem adotar cautela no tratamento de anexos, links, mensagens suspeitas, solicitações financeiras, compartilhamento de informações sigilosas e tentativas de phishing. O ambiente de e-mail poderá ser monitorado, nos limites legais e regulatórios aplicáveis, para prevenção, detecção e resposta a ameaças como spam, malware, phishing, vazamento de dados e uso indevido.

6. USO DA INTERNET

O acesso à internet deve apoiar exclusivamente as atividades profissionais e observar os interesses da GESTORA. É vedado acessar, armazenar, divulgar ou compartilhar conteúdo ilegal, discriminatório, ofensivo, malicioso, não autorizado ou incompatível com o ambiente corporativo. A navegação poderá ser monitorada e controlada por soluções de segurança, com o objetivo de proteger os ativos tecnológicos, prevenir incidentes e assegurar a conformidade com esta política.

7. POLÍTICA DE SENHAS E CREDENCIAIS

- Credenciais são pessoais, intransferíveis e devem ser mantidas em sigilo.
- Senhas devem possuir complexidade compatível com o risco do ambiente e não devem ser reutilizadas em serviços pessoais ou externos.
- O compartilhamento de senhas, tokens, códigos de autenticação ou qualquer outro fator de acesso é proibido.
- Contas privilegiadas devem possuir controles adicionais, como autenticação multifator, registro de atividades e revisão periódica de permissões.
- Sempre que houver suspeita de comprometimento, a senha deve ser alterada imediatamente e o incidente comunicado à área responsável.

8. BACKUP, RETENÇÃO E RECUPERAÇÃO

Os processos de backup devem ser executados periodicamente para assegurar a recuperação de informações críticas em caso de falhas, incidentes, exclusões indevidas, indisponibilidade ou eventos de segurança. Os backups devem possuir critérios definidos de periodicidade, retenção, proteção contra alteração indevida, testes de restauração e segregação adequada, conforme os requisitos de negócio, legais e regulatórios aplicáveis.

9. PROTEÇÃO CONTRA MALWARE E AMEAÇAS

Todos os ativos corporativos devem possuir mecanismos de proteção contra malware, ransomware, exploração de vulnerabilidades e softwares não autorizados. As soluções de segurança devem permanecer ativas, atualizadas e monitoradas. A instalação, remoção ou alteração de softwares de segurança somente poderá ser realizada por equipe autorizada, mediante justificativa e registro

apropriado.

10. AMBIENTE EM NÚVEM

O uso de serviços em nuvem deve observar controles de identidade, autenticação multifator, gestão de dispositivos, classificação da informação, proteção contra vazamento de dados, monitoramento de atividades e revisão periódica de permissões. O acesso aos recursos corporativos deve ocorrer por dispositivos autorizados, protegidos e aderentes aos padrões mínimos de segurança definidos pela organização.

11. PREVENÇÃO CONTRA PERDAS E DANOS

A GESTORA deve manter controles de prevenção contra perda de dados para identificar, monitorar e restringir o compartilhamento indevido de informações confidenciais, estratégicas, financeiras, pessoais ou sensíveis. Tais controles devem abranger e-mail, armazenamento em nuvem, compartilhamento de arquivos, dispositivos e demais canais corporativos, respeitando os limites legais e regulatórios aplicáveis.

12. CONTINUIDADE DE NEGÓCIOS E RESPOSTAS A INCIDENTES

Os serviços críticos devem ser suportados por procedimentos de continuidade de negócios, contingência, recuperação e resposta a incidentes. Incidentes de segurança devem ser comunicados imediatamente aos responsáveis, registrados, classificados, tratados e acompanhados até sua conclusão, incluindo análise de causa, ações corretivas e medidas preventivas para redução de recorrência.

13. CONFORMIDADE LEGAL, TREINAMENTO E VALIDADE

Todos os colaboradores, prestadores de serviços e partes aplicáveis devem observar a legislação vigente, obrigações contratuais, normas internas e requisitos regulatórios relacionados à segurança da informação e proteção de dados. Treinamentos e ações de conscientização devem ser realizados periodicamente. Esta política deve ser revisada, no mínimo, a cada 24 meses ou sempre que houver mudanças relevantes no ambiente tecnológico, regulatório, organizacional ou de riscos.

Histórico das atualizações		
DATA	**VERSÃO**	**RESPONSÁVEL**
Julho de 2026	1ª	Atual IT