1º TABELIÃO DE NOTAS E REGISTROS DE IMÓVEIS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PSI - 2026

1º Tabelionato de Notas e Registro de Imóveis de Miracema-TO

Elaborado por:
SimplifiCart - DPO da Serventia

Versão 1.0

Miracema-TO, Fevereiro de 2026

Histórico de Versões

Esta política é revisada com periodicidade anual ou sempre que assim entenderem os gestores. A presente política é elaborada pela equipe técnica da SimplifiCart, na qualidade de DPO contratado, com o apoio da equipe técnica do cartório, sendo posteriormente revisada e aprovada pela alta direção da serventia, representada pelo próprio titular ou por comitê interno que o represente.

DATA	VERSÃO	DESCRIÇÃO	AUTOR	APROVAÇÃO
04/02/2026	1.0	Política de Segurança da Informação	SimplifiCart - Equipe Técnica de Elaboração	Alta Direção do Cartório

Sumário

1. Introdução

A Política de Segurança da Informação, doravante denominada PSI, é o documento que orienta e estabelece as diretrizes institucionais do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** para a proteção dos ativos de informação e a mitigação de riscos e responsabilidades legais, aplicando-se a todos os colaboradores, prestadores de serviço, fornecedores e demais partes que tenham acesso às informações da serventia.

A observância desta Política é obrigatória e sua aplicação se estende a todas as áreas da instituição, devendo ser incorporada às rotinas operacionais e administrativas do Cartório.

A presente PSI fundamenta-se nas recomendações da norma ABNT NBR ISO/IEC 27002, reconhecida internacionalmente como código de boas práticas para a gestão da segurança da informação, estando também em conformidade com a legislação vigente aplicável à matéria no Brasil.

As diretrizes desta Política foram elaboradas com base nas seguintes normas e boas práticas de segurança da informação:

- ABNT NBR ISO/IEC 27002
- ABNT NBR 15999-1
- ABNT NBR 15999-2
- LEI Nº 13.709/2018 (LGPD)
- PROVIMENTO 74/2018 do CNJ
- PROVIMENTO 149/2023 do CNJ

2. Objetivo

Esta Política de Segurança da Informação tem por objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas a serem observadas para a proteção das informações do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, abrangendo todos os ativos de informação sob sua responsabilidade.

A presente Política visa à preservação dos princípios da confidencialidade, disponibilidade, autenticidade e integridade da informação, por meio da adoção de mecanismos preventivos de controle físico e lógico, bem como ao atendimento às determinações do Conselho Nacional de Justiça – CNJ, em especial ao Provimento nº 74, de 31 de julho de 2018, Provimento 149, de 30 de setembro de 2023, e à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

3. Escopo

Instituir a Política de Segurança da Informação (PSI) no âmbito do 1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e critérios para a implementação de ações e controles destinados a assegurar a proteção das informações e dos dados pessoais, em conformidade com a legislação vigente, as normas do Conselho Nacional de Justiça – CNJ e as boas práticas de segurança da informação.

Esta Política aplica-se a todos os ativos de informação do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, abrangendo, entre outros, dados e documentos físicos ou digitais, sistemas de informação, aplicativos, bases de dados, dispositivos, redes, serviços em nuvem, meios de armazenamento, comunicações eletrônicas e demais recursos tecnológicos utilizados no desempenho das atividades da serventia.

A PSI é aplicável a todos os colaboradores, prepostos, funcionários, estagiários, contratados, parceiros, fornecedores e terceiros que tenham acesso, utilizem, tratem ou processem informações do Tabelionato, seja em ambiente interno ou externo, incluindo situações de acesso remoto, teletrabalho ou utilização de dispositivos pessoais (BYOD – Bring Your Own Device), desde que autorizados.

As disposições desta Política deverão ser observadas em todos os processos, rotinas e operações da serventia, servindo como referência para auditorias internas e externas, fiscalizações da Corregedoria e do CNJ, bem como para a apuração de incidentes de segurança da informação e de proteção de dados pessoais.

4. Glossário

Para a adequada compreensão dos termos utilizados nesta Política de Segurança da Informação, adotam-se as seguintes definições:

Agentes do Cartório: São todos os colaboradores, prepostos, estagiários, contratados, parceiros, fornecedores e terceiros que geram, acessam, tratam ou manipulam informações no âmbito do cartório.

Ativo: Qualquer elemento que possua valor para a organização, incluindo informações, processos, sistemas, pessoas, infraestrutura e imagem institucional. (ISO/IEC 13335-1:2004)

Ativo Crítico: Ativo que gera, armazena, processa, transmite ou descarta informações de alto valor e elevada criticidade para o negócio, cujo comprometimento pode causar impactos relevantes à serventia.

Autenticidade: Propriedade que assegura que a identidade de usuários, sistemas ou processos seja legítima e verificável.

Avaliação de Riscos: Processo global que compreende a identificação, análise e valoração dos riscos. (ABNT ISO/IEC Guia 73:2005)

Comitê Gestor de Segurança da Informação (CGSI): Grupo designado com a responsabilidade de promover, coordenar e acompanhar a implementação das ações de Segurança da Informação no âmbito do cartório.

Confidencialidade: Propriedade que assegura que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados. (ISO/IEC 13335-1:2004)

Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável, nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Dado Pessoal Sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme definição da LGPD.

Diretriz: Orientação que estabelece o que deve ser feito e como deve ser feito para o alcance dos objetivos definidos nas políticas institucionais. (ISO/IEC 27002:2005)

Disponibilidade: Propriedade que garante que a informação esteja acessível e utilizável, sob demanda, por uma entidade autorizada. (ISO/IEC 13335-1:2004)

Evento de Segurança da Informação: Ocorrência identificada em dispositivos, sistemas, serviços ou redes que possa indicar possível violação da Política de Segurança da Informação, falha de controles ou situação relevante para a segurança da informação. (ISO/IEC TR 18044:2004)

Gestão de Riscos: Conjunto de atividades coordenadas para dirigir e controlar a organização no que se refere aos riscos, incluindo avaliação, tratamento, aceitação e comunicação dos riscos. (ABNT ISO/IEC Guia 73:2005)

Incidente de Segurança da Informação: Evento único ou série de eventos indesejados ou inesperados que tenham alta probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação. (ISO/IEC TR 18044:2004)

Integridade: Propriedade que assegura a exatidão, completude e consistência da informação e dos meios necessários para seu tratamento ou acesso. (ISO/IEC 13335-1:2004)

Política de Segurança da Informação (PSI): Documento que expressa o comprometimento da alta direção e estabelece as diretrizes para o gerenciamento da Segurança da Informação, devendo ser aprovado, divulgado e comunicado às partes interessadas. (ISO/IEC 27002:2005)

Proprietário da Informação: Agente do cartório responsável por definir quem pode acessar determinada informação, bem como os níveis e privilégios de acesso.

Regras Operacionais: Conjunto de instruções que orientam os usuários quanto ao uso adequado dos recursos de Tecnologia da Informação e Comunicação.

Recursos de Tecnologia da Informação e Comunicação (TIC): Conjunto de dispositivos, equipamentos, sistemas, softwares, redes e demais recursos tecnológicos utilizados para o processamento, armazenamento, transmissão ou acesso a dados e informações.

Salvaguarda de Processo Crítico: Conjunto de ações essenciais para assegurar a continuidade de processos vitais do cartório, evitando falhas que possam gerar prejuízos operacionais, financeiros, reputacionais ou comprometer a continuidade do negócio.

Segurança da Informação: Preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação, podendo envolver ainda princípios como responsabilidade, não repúdio e confiabilidade. (ABNT NBR ISO/IEC 17799:2005)

Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, nos termos da LGPD.

Tratamento de Riscos: Processo de seleção e implementação de medidas de controle para modificar ou reduzir riscos identificados. (ABNT ISO/IEC Guia 73:2005)

Usuário: Pessoa física autorizada a utilizar sistemas e/ou recursos de Tecnologia da Informação e Comunicação do cartório.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme definido na LGPD.

5. Segurança da Informação

A informação constitui um dos principais patrimônios das organizações na atualidade. Um fluxo informacional eficiente, seguro e confiável é fator determinante para a continuidade, a credibilidade e o sucesso das atividades institucionais. Contudo, o avanço tecnológico e a crescente facilidade de acesso à informação transformam esse ativo estratégico em alvo constante de ameaças internas e externas.

Quando não gerenciados de forma adequada, os riscos e as ameaças à segurança da informação podem ocasionar danos relevantes ao **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, comprometendo não apenas suas operações, mas também sua reputação institucional e a confiança dos usuários dos serviços prestados.

Diante desse cenário, o **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** institui a presente Política de Segurança da Informação (PSI), que estabelece o alicerce das ações e controles voltados à proteção de seus ativos de informação, em consonância com a legislação vigente, as normas do Conselho Nacional de Justiça e as boas práticas de segurança da informação.

A Segurança da Informação compreende um conjunto contínuo de esforços destinados à proteção dos ativos informacionais da serventia, contribuindo para o cumprimento de sua missão institucional e para a prestação de serviços com segurança, confiabilidade e transparência. Para tanto, esta Política busca assegurar os seguintes objetivos fundamentais:

- **Confidencialidade:** garantir que as informações sejam acessadas exclusivamente por pessoas devidamente autorizadas;
- **Integridade:** assegurar que as informações permaneçam íntegras, completas e livres de alterações indevidas, sejam elas acidentais ou intencionais;
- **Disponibilidade:** garantir que as informações estejam acessíveis às pessoas autorizadas sempre que necessário;
- **Autenticidade:** assegurar a identificação e o registro dos usuários que criam, acessam ou alteram informações, possibilitando a rastreabilidade das ações realizadas sobre os dados.

O presente documento estabelece as diretrizes a serem observadas no ambiente interno do Cartório, devendo toda informação ser protegida em conformidade com os princípios e disposições aqui definidos.

A adoção de práticas e procedimentos voltados à Segurança da Informação constitui prioridade permanente do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, com o objetivo de reduzir falhas, prevenir incidentes e minimizar impactos que possam comprometer sua imagem institucional ou causar prejuízos ao próprio Cartório e aos usuários de seus serviços.

O Cartório, por intermédio de seu Titular, bem como seus colaboradores, prepostos, prestadores de serviços e demais pessoas que, direta ou indiretamente, participem de suas atividades, comprometem-se a observar, aplicar e cumprir integralmente as disposições desta Política.

6. Política de Segurança da Informação

6.1 Proteção da Informação

A informação constitui um ativo essencial para a execução das atividades do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, sendo fundamental para a continuidade dos serviços, a segurança jurídica e a confiança dos usuários. Assim como os demais ativos da serventia, a informação deve ser devidamente manuseada, protegida e preservada.

A informação pode se apresentar sob diversas formas, incluindo, mas não se limitando a:

- Sistemas de informação;
- Diretórios de rede;
- Bancos de dados;
- Documentos em meio físico, magnético ou óptico;
- Dispositivos eletrônicos;
- Equipamentos portáteis e microfilmes;
- Comunicações orais relacionadas às atividades institucionais.

Toda informação relacionada às operações do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, produzida, recebida ou tratada no exercício de suas atividades, seja nas dependências da serventia ou em ambiente externo autorizado, constitui ativo institucional, indispensável à condução de suas funções e à sua própria existência.

Independentemente da forma de apresentação ou do meio pelo qual a informação seja criada, compartilhada, transmitida ou armazenada, seu uso deve restringir-se exclusivamente às finalidades para as quais foi autorizada, observando-se os princípios da necessidade e da finalidade.

A modificação, divulgação ou destruição não autorizadas de informações, decorrentes de erros, falhas operacionais, fraudes, vandalismo, espionagem ou sabotagem, podem causar danos relevantes à serventia, aos usuários dos serviços e à sua imagem institucional.

É diretriz que toda informação de propriedade ou sob a responsabilidade do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** seja protegida contra riscos e ameaças que possam comprometer sua confidencialidade, integridade, disponibilidade e autenticidade, nos termos desta Política de Segurança da Informação.

6.2 Responsabilidades

É dever e responsabilidade de todos os colaboradores do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, bem como de terceiros, como prestadores de serviços, fornecedores e parceiros, observar e cumprir as políticas, normas, procedimentos e orientações estabelecidos nesta Política de Segurança da Informação.

Todas as atividades executadas pelos colaboradores, bem como de terceiros, fornecedores e parceiros, devem observar rigorosamente a legislação vigente e as normas expedidas por órgãos e entidades reguladoras, no que se refere à Segurança da Informação e à proteção de dados.

Para apoiar o cumprimento desta Política, o **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** instituiu a área de Segurança da Informação, responsável por coordenar as práticas, controles e orientações relacionados à proteção dos ativos de informação.

Compete ao DPO da Serventia, em conjunto com a equipe de Tecnologia da Informação (TI) do Tabelionato, elaborar, manter e atualizar as políticas, normas e padrões de segurança, bem como apoiar os usuários na prevenção e no tratamento de incidentes relacionados à Segurança da Informação, em conformidade com esta Política.

6.2.1 Diretrizes da Segurança da Informação

As Diretrizes de Segurança da Informação constituem a base para a gestão da Segurança da Informação e orientam a elaboração da Política de Segurança da Informação, bem como das Normas e dos Procedimentos correlatos. Tais diretrizes devem ser observadas por todos os setores do cartório, de forma integrada e contínua.

Comitê Gestor de Segurança da Informação (CGSI)

Deverá ser instituído um Comitê Gestor de Segurança da Informação (CGSI), de caráter multidisciplinar, responsável por promover a cultura de Segurança da Informação no âmbito do cartório, bem como por elaborar a Política de Segurança da Informação e aprovar as Normas e os Procedimentos de Segurança da Informação.

O CGSI deverá ser composto por representantes dos setores que tratam ativos críticos para o negócio e terá, entre outras, as seguintes atribuições:

- Apoiar as ações estratégicas necessárias à implantação dos processos mínimos definidos no Modelo de Gestão de Segurança da Informação;
- Constituir grupos de trabalho para tratar temas específicos e propor soluções relacionadas à Segurança da Informação, avaliando, inclusive, a necessidade de criação de área específica para sua gestão;
- Propor alterações e atualizações na Política de Segurança da Informação;
- Propor normas e procedimentos relacionados à Segurança da Informação.

Modelo de Gestão da Segurança da Informação

Deverá ser estabelecido um Modelo de Gestão que possibilite a criação, implementação e manutenção de um Sistema de Gestão de Segurança da Informação (SGSI), apoiado por Política, Normas e Procedimentos de Segurança da Informação. O Modelo de Gestão deverá contemplar, no mínimo, os seguintes processos:

- Planejamento estratégico da Segurança da Informação;
- Gestão da Política de Segurança da Informação, das Normas e dos Procedimentos;
- Classificação da informação e definição dos procedimentos de acesso e tratamento;
- Controle dos procedimentos de proteção da integridade dos ambientes de informatização, internos, externos e portáteis;
- Controle de acesso lógico e físico;
- Gestão de riscos;
- Gestão da continuidade do negócio;
- Gestão de resposta a incidentes de Segurança da Informação;
- Gestão de mudanças;
- Divulgação, capacitação e conscientização;
- Auditoria e conformidade.

Sistema de Gestão de Segurança da Informação (SGSI)

A implantação do SGSI, com base nos processos definidos no Modelo de Gestão, deverá possibilitar, no mínimo:

- A classificação e a gestão das informações, permitindo o inventário dos ativos informacionais, sua classificação conforme o nível de confidencialidade e a associação a um Proprietário da Informação;
- A avaliação contínua dos riscos de Segurança da Informação, por meio de análises sistemáticas e periódicas;
- A gestão de acesso lógico e físico aos sistemas de informação, garantindo que os acessos estejam alinhados às Normas e Procedimentos estabelecidos;
- A gestão de riscos em Segurança da Informação, com o objetivo de reduzir riscos a níveis aceitáveis, por meio da adoção de medidas de segurança adequadas;
- A gestão da continuidade do negócio, visando reduzir impactos decorrentes de falhas, incidentes ou desastres, especialmente nos ativos que suportam processos críticos do cartório;
- A validação e manutenção de evidências de cumprimento da Política de Segurança da Informação;
- O inventário e a gestão dos ativos de Tecnologia da Informação e Comunicação, com foco nos ativos críticos;
- A definição e utilização de Termos de Responsabilidade para o acesso às informações classificadas.

Estrutura Normativa da Segurança da Informação

Deverá ser estabelecida uma Estrutura Normativa de Segurança da Informação, composta, no mínimo, por:

Política de Segurança da Informação (PSI): documento que define a estrutura, os princípios, as diretrizes e as responsabilidades relacionadas à Segurança da Informação;

Normas de Segurança da Informação: documentos que estabelecem obrigações e requisitos a serem observados, abrangendo, no mínimo:

- Tratamento da Informação;
- Tratamento de Incidentes de Segurança da Informação;
- Prevenção e tratamento de códigos maliciosos;
- Controle de acesso lógico e físico aos sistemas de informação;
- Uso dos recursos de Tecnologia da Informação e Comunicação (internet, correio eletrônico, redes sociais, entre outros);
- Política de geração, armazenamento e restauração de cópias de segurança (backup).
- Procedimentos de Segurança da Informação: regras operacionais que detalham a execução das Normas de Segurança, permitindo sua aplicação prática nas rotinas do cartório.

Capacitação e Resposta a Incidentes

Deverá ser instituído um programa contínuo de capacitação e conscientização, voltado a todos os envolvidos nas operações do Cartório, incluindo colaboradores, fornecedores e terceiros autorizados, com foco na adoção de comportamentos seguros no uso das informações.

Deverá ser implantada uma equipe de resposta a incidentes de Segurança da Informação, responsável por avaliar fragilidades, tratar eventos de segurança e apoiar a adoção de ações corretivas em tempo hábil, especialmente em relação aos ativos críticos de Tecnologia da Informação e Comunicação.

6.3 Confidencialidade da Informação

Para os fins desta Política de Segurança da Informação, consideram-se informações confidenciais todas as informações não disponíveis ao público ou classificadas como reservadas, incluindo, mas não se limitando a: dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais de apoio, projetos, estudos, documentos e quaisquer outros registros, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentações de computador, bem como comunicações realizadas por escrito, verbalmente ou por qualquer outro meio.

São igualmente consideradas confidenciais todas as informações produzidas, recebidas, tratadas ou reveladas pelo **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, bem como aquelas obtidas em razão do exercício de atividades profissionais, contratuais ou do vínculo funcional mantido com a serventia.

São responsáveis pela observância desta Política, no que lhes couber:

- o titular da serventia;
- os escreventes;
- os colaboradores em geral (analistas, auxiliares, aprendizes, estagiários e demais prepostos);
- os consultores e terceiros autorizados, incluindo advogados, auditores e consultores de Tecnologia da Informação (TI);
- os fornecedores e prestadores de serviços que tenham acesso, direto ou indireto, a informações do cartório, incluindo, mas não se limitando a:
  - empresas fornecedoras de sistemas de automação cartorária;
  - serviços de contabilidade;
  - empresas de segurança e saúde do trabalho;

- serviços terceirizados de recursos humanos (RH);
- empresas responsáveis pela realização de notificações de protesto;
- demais empresas contratadas que, no exercício de suas atividades, tratem, armazenem, processem ou tenham acesso a informações sob a responsabilidade do cartório.

Os colaboradores, consultores e fornecedores que tiverem acesso a informações confidenciais deverão mantê-las sob estrito sigilo, restringindo seu uso exclusivamente às finalidades autorizadas, bem como limitar e controlar o acesso, inclusive quanto à reprodução, cópia, extração ou qualquer outra forma de compartilhamento das informações.

É vedada a divulgação, cessão ou repasse de informações confidenciais a terceiros sem o prévio e expresso consentimento, por escrito, do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, ressalvadas as hipóteses legalmente previstas. Toda e qualquer revelação de informação deverá observar rigorosamente os termos e condições definidos pela serventia.

As informações confidenciais somente poderão ser utilizadas para a execução das atividades profissionais ou contratuais previamente autorizadas, sendo expressamente proibido seu uso para quaisquer outras finalidades diversas.

O colaborador, consultor ou fornecedor deverá adotar todas as medidas necessárias para resguardar as informações confidenciais, responsabilizando-se por eventual descumprimento desta Política por parte de seus representantes legais, empregados ou pessoas sob sua supervisão.

Qualquer uso indevido, acesso não autorizado, perda, vazamento ou divulgação irregular de informações confidenciais deverá ser comunicado imediatamente ao **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, para adoção das medidas cabíveis.

Exceções à Obrigação de Confidencialidade

Não se aplica a obrigação de confidencialidade prevista nesta Política nas seguintes hipóteses:

- cumprimento de determinações legais ou ordens emanadas do Poder Judiciário, do Poder Legislativo, de Tribunais ou de órgãos da Administração Pública competente;
- compartilhamento de informações confidenciais com agentes, representantes ou fornecedores autorizados do cartório (incluindo advogados, procuradores, auditores, consultores e prestadores de serviços), desde que estritamente necessário ao exercício de suas funções;
- divulgação de informações mediante consentimento prévio e expresso, por escrito, do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**.

Responsabilidade e Ciência

As cláusulas de ciência, responsabilidade e confidencialidade têm por finalidade alertar e responsabilizar colaboradores, consultores e fornecedores de que o acesso, o uso e o manuseio das informações devem restringir-se exclusivamente ao desempenho das atribuições funcionais ou contratuais, sendo vedada sua utilização para qualquer finalidade diversa daquela previamente autorizada.

6.4. Violação da Política, Normas e Procedimentos de Segurança da Informação

Toda violação, suspeita de violação ou não conformidade em relação a esta Política de Segurança da Informação, bem como às normas e procedimentos dela decorrentes, deverá ser comunicada imediatamente à área de Segurança da Informação e/ou ao superior imediato.
As ocorrências serão analisadas e investigadas, com a finalidade de identificar causas e definir medidas corretivas e preventivas, incluindo a correção de falhas ou o aprimoramento de processos.
Poderão ensejar sanções, entre outras, as seguintes condutas:

- uso não autorizado ou ilegal de softwares;
- introdução, intencional ou não, de códigos maliciosos;
- tentativa de acesso não autorizado a dados ou sistemas;
- compartilhamento ou divulgação indevida de informações sensíveis ou de clientes.

O descumprimento desta Política sujeitará os responsáveis às sanções administrativas cabíveis, sem prejuízo da responsabilização civil e criminal, nos termos da legislação vigente, inclusive com a rescisão contratual, quando aplicável.
Em caso de dúvidas, o interessado deverá procurar o responsável pela Tecnologia da Informação (TI) ou seu superior imediato.

7. Princípios e Diretivas da Política de Segurança da Informação

7.1. Classificação da Informação

As informações e os ativos de informação, incluindo sistemas de informação, diretórios de rede e bancos de dados, são classificados como estritamente confidenciais. As informações devem ser tratadas de forma adequada em todas as etapas do seu ciclo de vida, compreendendo a geração, o armazenamento, o uso, a transferência e o descarte, observando-se as diretrizes desta Política.

As informações confidenciais exigem sigilo absoluto, devendo ser protegidas contra acessos, alterações, divulgações ou destruições não autorizadas, bem como disponibilizadas exclusivamente às pessoas devidamente autorizadas, apenas quando necessário ao desempenho de suas funções.

Cabe a todos os colaboradores, consultores, fornecedores e terceiros autorizados adotar as medidas e os cuidados necessários para a proteção dessas informações.

Falhas na confidencialidade, integridade ou disponibilidade das informações confidenciais podem acarretar prejuízos significativos ao **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, incluindo perdas financeiras, comprometimento da produtividade, da competitividade e da imagem institucional, podendo, em casos extremos, ocasionar graves impactos às operações da serventia.

São exemplos de informações confidenciais, entre outras:

- informações de clientes protegidas por obrigação legal, incluindo dados cadastrais (CPF, RG, entre outros) e informações financeiras;
- informações sobre produtos, serviços e processos que representem vantagem competitiva do Tabelionato;
- materiais estratégicos do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, independentemente do meio em que se encontrem (impresso, digital, sistemas, comunicações eletrônicas ou conhecimento institucional);
- informações internas que não devam ser divulgadas ao público externo antes de sua divulgação oficial pelas áreas competentes;
- credenciais de acesso (certificado digital), senhas de sistemas, redes e estações de trabalho, as quais são pessoais, sigilosas e intransferíveis.

7.2. Acesso a Sistemas e Recursos de Rede

Cada colaborador é integralmente responsável pela guarda, confidencialidade e uso adequado de suas credenciais de acesso, incluindo senhas, bem como por todas as ações realizadas a partir de sua utilização. As autorizações de acesso aos sistemas e a definição de perfis deverão ser concedidas pelo superior imediato, podendo contar com o apoio técnico da área de Tecnologia da Informação (TI).

O acesso e o uso de sistemas de informação, diretórios de rede, bancos de dados e demais recursos tecnológicos devem ser restritos exclusivamente a pessoas previamente autorizadas e limitados à necessidade estrita para o desempenho de suas atribuições.

Acessos desnecessários, indevidos ou com privilégios excessivos deverão ser imediatamente revogados. A concessão de acessos deverá observar o princípio do menor privilégio, garantindo apenas o nível mínimo necessário para a execução da função.

Os acessos concedidos deverão ser revisados periodicamente pelo superior imediato, com o apoio da área de TI, quando necessário.

7.3. Utilização dos Recursos de Informação

Somente equipamentos, sistemas e softwares disponibilizados, autorizados ou homologados pelo **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** poderão ser instalados ou conectados à sua rede e aos seus ambientes de informação.

Todos os ativos de informação devem ser devidamente protegidos e armazenados de forma segura, especialmente documentos físicos e mídias removíveis. Documentos não deverão ser deixados expostos ou abandonados após sua impressão, cópia ou utilização, devendo ser guardados ou descartados de forma adequada, conforme as diretrizes desta Política.

7.4. Autenticação e Senhas

Cada colaborador é responsável por todos os atos realizados com o uso de seu identificador de acesso (login e senha), que é único, pessoal e intransferível, destinado à identificação e autenticação no acesso às informações e aos recursos de tecnologia.

Os colaboradores devem:

- manter a senha sob sigilo absoluto, não a compartilhando nem registrando;
- alterá-la sempre que houver suspeita de comprometimento;
- utilizar senhas de difícil adivinhação;
- impedir o uso do equipamento por terceiros enquanto estiver autenticado;
- bloquear o equipamento ao se ausentar do posto de trabalho.

7.5. Direito de Acesso (Autorização)

A concessão de acesso às informações e aos sistemas deve ocorrer exclusivamente por necessidade funcional, sendo os acessos pessoais e intransferíveis.

O superior imediato é responsável pela solicitação e acompanhamento dos acessos atribuídos aos colaboradores, estagiários, prestadores de serviços, e terceiros sob sua supervisão, respondendo por eventuais usos inadequados decorrentes das autorizações concedidas.

7.6. Direitos de Propriedade

Todo produto resultante das atividades desenvolvidas por colaboradores e/ou consultores, incluindo dados, documentos, sistemas, metodologias e demais materiais, é de propriedade exclusiva do **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO.**

Em caso de desligamento ou rescisão contratual, o colaborador ou consultor deverá devolver todas as informações confidenciais sob sua posse ou declarar formalmente sua destruição, conforme orientações da serventia.

7.7. Equipamentos Particulares / Privados

Equipamentos particulares ou privados não devem ser utilizados para armazenar ou processar informações do cartório, salvo mediante autorização prévia da área de Tecnologia da Informação (TI).

Os responsáveis por tais equipamentos deverão garantir que estejam protegidos, atualizados e livres de ameaças, incluindo a utilização de antivírus adequado.

7.8. Mesa Limpa e Organização do Ambiente de Trabalho

Nenhuma informação confidencial deve permanecer exposta, seja em documentos físicos ou em dispositivos eletrônicos.

Ao usar uma impressora coletiva, recolher o documento impresso imediatamente, e os dados contendo informações confidenciais ou sigilosas deverão ser descartados de forma segura, preferencialmente por fragmentação.

7.9. Conversas em Locais Públicos e Registro de Informações

É vedada a discussão ou divulgação de informações confidenciais em locais públicos, redes sociais ou aplicativos de mensagens, salvo quando expressamente autorizado e estritamente necessário ao desempenho das atividades, com ciência da administração do cartório.

8. Sansões Disciplinares

As violações desta Política de Segurança da Informação, ainda que decorrentes de omissão, tentativa não consumada ou descumprimento parcial, bem como das demais normas e procedimentos de segurança, poderão ensejar a aplicação de sanções disciplinares, que incluem advertência verbal, advertência por escrito, suspensão não remunerada e, quando cabível, o encerramento do vínculo empregatício ou contratual com o **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**.

A aplicação das sanções será realizada após análise da gestão, considerando-se a gravidade da infração, os efeitos produzidos, a recorrência e as disposições previstas na legislação trabalhista vigente, em especial a Consolidação das Leis do Trabalho (CLT), ou outro instrumento legal aplicável à pessoa envolvida.

No caso de terceiros contratados, fornecedores ou prestadores de serviços, a ocorrência será analisada pela gestão do Cartório, que deliberará sobre a aplicação das sanções cabíveis, nos termos previstos nos respectivos contratos, aditivos ou instrumentos de confidencialidade.

Nas hipóteses em que a violação caracterizar atividade ilícita ou resultar em dano material, moral ou reputacional ao **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO**, o responsável poderá ser civil, administrativa e criminalmente responsabilizado, sem prejuízo da adoção das medidas judiciais cabíveis.

Casos Omissos

Os casos omissos ou situações não previstas expressamente nesta Política serão avaliados pela gestão do Cartório, para posterior deliberação.

Ressalta-se que as diretrizes estabelecidas nesta Política e nas demais normas de segurança não se esgotam, em razão da constante evolução tecnológica e do surgimento contínuo de novas ameaças à segurança da informação, podendo ser atualizadas sempre que necessário.

9. Aprovação e Publicação

Com o objetivo de conferir segurança jurídica, efetividade e validade à presente Política de Segurança da Informação (PSI), o **1º Tabelionato de Notas e Registros de Imóveis de Miracema-TO** formaliza sua aprovação mediante as assinaturas das seguintes autoridades:

- Responsável pela Elaboração da Política de Segurança da Informação;
- Encarregado pelo Tratamento de Dados Pessoais (DPO);
- Controlador ou Comitê Interno, na qualidade de representante da alta administração da serventia.

A serventia reconhece que o ambiente tecnológico, normativo, institucional e regulatório é dinâmico e sujeito a constantes mudanças. Dessa forma, reafirma seu compromisso com a Segurança da Informação, comprometendo-se a realizar a avaliação e a revisão periódica desta Política, no mínimo anualmente, ou sempre que houver alterações relevantes nos processos internos, nos riscos identificados ou no marco regulatório aplicável.

A Política de Segurança da Informação (PSI) encontra-se disponível para consulta pública no site oficial do cartório **(https://cartoriomiracema.com.br/)**, bem como por meio de QR Code afixado no balcão de atendimento da serventia.

Este documento entra em vigor na data de sua publicação.

Miracema-TO, 4 de Fevereiro de 2025.

QUADRO DE ASSINANTES	
Responsável pela Elaboração	SimplifiCart (Equipe Téc. de Elaboração e DPO)
Encarregado:	Ludimilla Cantareli Moura Almeida
Controlador ou Comitê Interno (Representante do Controlador)	Vágmo Pereira Batista

MANIFESTO DE ASSINATURAS

Código de validação: YZ7QK-VRTGT-7JZZY-FVCMK

Documento assinado com o uso de certificado digital ICP Brasil, no Assinador Registro de Imóveis, pelos seguintes signatários:

Ludimilla Cantareli Moura Almeida (CPF 027.083.481-83)

Ludimilla Cantareli Moura Almeida (CPF 027.083.481-83)

VÁGMO PEREIRA BATISTA (CPF 774.098.921-53)

Para verificar as assinaturas, acesse o link direto de validação deste documento:

https://assinador.registrodeimoveis.org.br/validate/YZ7QK-VRTGT-7JZZY-FVCMK

Ou acesse a consulta de documentos assinados disponível no link abaixo e informe o código de validação:

https://assinador.registrodeimoveis.org.br/validate