CARTÓRIO COELHO AMORIM

TABELIONATO DE NOTAS, DE PROTESTO DE TÍTULOS, TABELIONATO E OFICIALATO DE REGISTRO DE CONTRATOS MARÍTIMOS

(Protesto de Títulos reservado até a vacância)

COMARCA DE ITAPURANGA – ESTADO DE GOIÁS

Titular: TALITHA DURÃES COELHO AMORIM

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Art. 1º - Esta Política estabelece as diretrizes e controles de segurança da informação para proteção dos dados pessoais, dos atos notariais e registrais, em conformidade com o Provimento CNJ nº 213/2026, a Lei nº 13.709/18 (LGPD) e a Lei nº 8.935/94.

Parágrafo único - Esta política visa proteger o acervo notarial e registral contra acessos não autorizados, vazamentos de dados e ataques cibernéticos, garantindo a rastreabilidade e a autoria de todas as ações realizadas nos sistemas da serventia.

2. ABRANGÊNCIA

Art. 2º - Aplica-se a todos os colaboradores diretos, escreventes, prepostos, estagiários, prestadores de serviços terceirizados (incluindo equipe de suporte técnico) que possuam acesso à rede, aos computadores, aos sistemas ou a quaisquer dados e informações tratados no âmbito do Tabelionato.

3. GESTÃO DE RISCOS

Art. 3º - O Tabelionato manterá processo de gestão de riscos de segurança da informação, com avaliações periódicas para identificar ameaças e vulnerabilidades em seus sistemas, conforme as melhores práticas de governança e as orientações do Provimento CNJ nº 213/2026.

4. PRINCÍPIOS DE SEGURANÇA

Art. 4º - A segurança da informação no Tabelionato será regida pelos princípios da:

- **Confidencialidade**: garantia de que a informação seja acessível apenas por pessoas autorizadas;
- **Integridade**: salvaguarda da exatidão e completeza da informação;
- **Disponibilidade**: garantia de que a informação esteja acessível quando necessário;
- **Autenticidade**: certeza da identidade de quem realiza o ato;
- **Irretratabilidade**: impossibilidade de negar a autoria de um ato praticado

5. CONTROLES TÉCNICOS IMPLEMENTADOS

5.1. CONTROLE DE ACESSO LÓGICO

Art. 5º - O acesso aos sistemas eletrônicos será controlado e individualizado, nos termos do Provimento CNJ nº 213/2026.

I - Identificação única e intransferível para cada usuário (notário, escreventes, estagiários, suporte técnico), sendo vedado o uso de usuários genéricos (ex: "atendimento", "recepcao");

II - Utilização de senha complexa, com política de troca periódica, sendo vedado o compartilhamento de credenciais;

III - Bloqueio automático da sessão após período de inatividade (máximo de 5 minutos), devendo o colaborador bloquear manualmente a máquina (Tecla Windows + L) sempre que se ausentar;

IV - Registro de logs de auditoria com a individualização das ações realizadas no sistema, permitindo a rastreabilidade completa.

5.2. AUTENTICAÇÃO MULTIFATOR (MFA)

Art. 6º - O acesso a funções administrativas do sistema do cartório, bancos de dados, servidores e gerenciadores de rede deverá, obrigatoriamente, exigir autenticação multifator (MFA/2FA), conforme exigência do Provimento CNJ nº 213/2026 para acesso remoto e funções críticas.

5.3. PROTEÇÃO E INTEGRIDADE DOS DADOS

Art. 7º - Serão adotadas medidas para garantir a inviolabilidade, a conservação e a integridade dos dados e informações.

I - **Assinatura Digital**: Todos os atos notariais e registrais serão assinados digitalmente com certificado ICP-Brasil do notário, garantindo a autenticidade, a integridade e a irretratabilidade;

II - **Criptografia**: Utilização de criptografia em trânsito com protocolo TLS 1.2 ou superior e, para dados críticos armazenados, criptografia em repouso com padrão equivalente a AES-256 ou superior;

III - **Imutabilidade do Registro**: Garantia de que o ato eletrônico, uma vez assinado e registrado, não poderá ser alterado, preservando sua integridade.

5.4. SISTEMAS ELETRÔNICOS E INTERABILIDADE

Art. 8º - O Tabelionato utilizará sistemas eletrônicos homologados que atendam aos padrões de interoperabilidade estabelecidos pelo CNJ e pela Corregedoria-Geral da Justiça de Goiás.

I - Integração com os sistemas nacionais notariais e de registro (CENSEC, CESDI, RCTO);

II - Garantia de que os sistemas permitam a exportação de dados em formatos abertos e estruturados, quando aplicável;

III - Os sistemas serão submetidos a testes periódicos de vulnerabilidade e segurança.

5.5. BACKUP E RECUPERAÇÃO DE DESASTRES

Art. 9º - Será mantido regime de cópia de segurança (backup) para garantia da disponibilidade e recuperação das informações, conforme exigência do Provimento CNJ nº 213/2026.

I - Backup automático e diário de toda a base de dados e documentos digitais;

II - Armazenamento das cópias de segurança em local fisicamente distinto da serventia (off-site);

III - Realização de testes periódicos de restauração (no mínimo semestrais) para verificar a eficácia dos procedimentos e a integridade dos dados;

IV - Política de retenção definida, observando os prazos legais de guarda documental.

Art. 9º-A - O Tabelionato manterá formalizados:

I - **Plano de Continuidade de Negócios (PCN)** : conjunto de procedimentos para assegurar a continuidade da prestação dos serviços em situações de indisponibilidade;

II - **Plano de Recuperação de Desastres (PRD)** : medidas técnicas e operacionais para restauração de sistemas e dados após incidente grave;

III - **Definição de RTO e RPO**: serão estabelecidos formalmente os objetivos de tempo de recuperação (RTO) e ponto máximo de perda de dados aceitável (RPO), compatíveis com a classe da serventia;

IV - **Testes anuais**: os planos serão testados e revisados anualmente, com registro documental.

Art. 9º-B - O Tabelionato assegurará, contratual e tecnicamente:

I - **Reversibilidade**: garantia de restituição integral e utilizável dos dados, configurações e registros da serventia ao seu titular, em caso de encerramento contratual, substituição de fornecedor ou transição de gestão;

II - **Portabilidade**: possibilidade de extração, transferência e reutilização estruturada dos dados da serventia em formato interoperável, sem perda de integridade, rastreabilidade ou autenticidade;

III - **Simulação documentada**: será realizada simulação de extração integral do acervo, com periodicidade definida, mantendo-se registro dos testes.

5.6. PROTEÇÃO DE REDE E PREVENÇÃO CONTRA MALWARES

Art. 10 - Serão implementadas medidas técnicas para prevenção, detecção e resposta a incidentes cibernéticos.

I - Instalação e atualização permanente de software antivírus corporativo em todos os computadores e servidores, com proteção e atualizações em tempo real;

II - Utilização de firewall de borda (pfSense ou similar) para proteção da rede interna, bloqueando tentativas de intrusão externa e filtrando o acesso a sites maliciosos;

III - Monitoramento contínuo dos servidores, com geração de alertas automáticos em caso de anomalias;

IV - Manutenção de política de atualizações de segurança (patch management) para sistemas operacionais e aplicativos.

5.7. USO DE DISPOSITIVOS REMOVÍVEIS

Art. 11 - O uso de dispositivos removíveis (Pen Drives, HDs externos, cartões de memória) será restrito e monitorado, visando evitar a introdução de ransomwares e malwares na rede.

I - Dispositivos não identificados ou de origem pessoal terão seu uso bloqueado;

II - Quando necessário, o uso deverá ser autorizado previamente e o dispositivo submetido a verificação de segurança.

6. CONTROLES ADMINISTRATIVOS E FÍSICOS

6.1. TREINAMENTO E CONSCIENTIZAÇÃO

Art. 12º - Além dos controles técnicos, será promovida capacitação periódica dos colaboradores sobre os procedimentos de segurança, uso ético dos sistemas e identificação de ameaças (phishing, engenharia social).

6.2. CONTROLE FÍSICO

Art. 13 - O acesso às salas que abrigam servidores, equipamentos de rede e documentos físicos será restrito a pessoas autorizadas, com controle de entrada e saída.

6.3. GESTÃO DE DOCUMENTOS

Art. 14 - A destinação de documentos físicos e mídias de armazenamento será feita de forma segura, promovendo sua eliminação por meio de processos que impossibilitem a recuperação não autorizada de dados (fragmentação, destruição mecânica).

7. TRATAMENTO DE INCIDENTES DE SEGURANÇA

Art. 15 - Em conformidade com a LGPD e o Provimento CNJ nº 213/2026, qualquer incidente de segurança deverá ser tratado com urgência.

§1º - Notificação Imediata: Se um colaborador suspeitar de vazamento de senhas, infecção por vírus, acesso indevido ou qualquer outra anomalia, deverá notificar **imediatamente** a Tabeliã e o responsável técnico (STI).

§2º - Monitoramento Contínuo: A equipe de suporte técnico realizará o monitoramento ativo dos servidores e sistemas, com registro formal de incidentes detectados.

§3º - Comunicação à Corregedoria: Em caso de incidente de segurança que comprometa a disponibilidade, integridade ou confidencialidade dos dados da serventia, a Tabeliã, com apoio técnico, comunicará à Corregedoria-Geral de Justiça no prazo máximo de **72 (setenta e duas) horas** da ciência do fato, conforme exigência do art. 48 da LGPD e do Provimento CNJ nº 213/2026.

§4º - Comunicação à ANPD: Quando exigido por lei, o incidente também será comunicado à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados.

8. USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

Art. 16 - Os equipamentos de informática e o acesso à internet são ferramentas de trabalho fornecidas pelo cartório para fins profissionais.

I - É proibido o download, instalação ou execução de softwares não homologados pela STI;

II - É proibido utilizar o e-mail corporativo do cartório para cadastros em serviços pessoais ou sites de entretenimento;

III - A rede do cartório é monitorada, e a privacidade no uso dos equipamentos corporativos submete-se às necessidades de auditoria e segurança da serventia;

IV - O acesso a sites de conteúdo impróprio ou não relacionados à atividade laborativa será bloqueado.

9. TERMO DE RESPONSABILIDADE

Art. 17 - Todos os colaboradores, prestadores de serviços e terceiros com acesso aos sistemas ou dados da serventia deverão assinar um **Termo de Conformidade e Responsabilidade**, atestando que leram, compreenderam e se comprometem a seguir esta Política de Segurança da Informação.
Parágrafo único - Os termos assinados serão mantidos em arquivo organizado, podendo ser exigidos pela Corregedoria ou órgãos fiscalizadores.

10. DISPOSIÇÕES FINAIS

Art. 18 - O descumprimento desta Política sujeitará os infratores às sanções administrativas disciplinares cabíveis, podendo ensejar, conforme o caso, responsabilização civil ou penal.
Art. 19 - Esta Política será revisada anualmente, ou sempre que uma mudança significativa no ambiente de risco ou na legislação assim determinar.
Art. 20 - Esta Política entra em vigor na data de sua publicação, revogando as disposições em contrário.

Itapuranga-GO, 26 de fevereiro de 2026.

_____

Talitha Durães Coelho Amorim

Tabeliã Titular

gov.br Documento assinado digitalmente
SAVIO PEREIRA ALVES
Data: 27/03/2026 17:43:46-0300
Verifique em https://validar.iti.gov.br

_____

Savio Pereira Alves

Responsável Técnico - **STI**

Versão	Data	Alterações	Responsável
1.0	17/06/2025	Criação da Política (Prov. 74/2018)	Tabelião
2.0	26/02/2026	**Adequação ao Provimento CNJ nº 213/2026 e à LGPD:** • Autenticação Multifator (MFA) para funções críticas • Backup off-site com testes semestrais de restauração • Comunicação de incidentes à Corregedoria em 72h • Restrição e monitoramento de dispositivos removíveis • Monitoramento contínuo de servidores (10/10min) • Logs de auditoria individualizados e imutáveis • Bloqueio automático por inatividade (5 min) • Termo de responsabilidade obrigatório	Tabelião / STI

CARTÓRIO COELHO AMORIM

TERMO DE CONFORMIDADE E RESPONSABILIDADE
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Eu, _____, portador(a) do CPF nº _____, no exercício do cargo/função de _____ no Tabelionato de Notas, de Protesto de Títulos, Tabelionato e Oficialato de Registro de Contratos Marítimos de Itapuranga - Goiás, **DECLARO** que:

1. Estou ciente e compreendi plenamente as disposições contidas na **Política de Segurança da Informação** adotada por esta serventia;
2. Comprometo-me a cumprir rigorosamente todos os procedimentos estabelecidos, especialmente no que diz respeito a:
    - Uso individual e intransferível de minhas credenciais de acesso;
    - Não compartilhamento de senhas;
    - Bloqueio da estação de trabalho quando ausente;
    - Comunicação imediata de qualquer incidente de segurança;
    - Uso aceitável dos recursos tecnológicos;
3. Reconheço que:
    - O descumprimento das normas de segurança pode acarretar sanções administrativas, civis e disciplinares;
    - Devo participar obrigatoriamente dos treinamentos periódicos sobre o tema;

- Todas as minhas dúvidas sobre os procedimentos foram devidamente esclarecidas;

4. Estou ciente de que este Termo de Conformidade integra meu registro funcional e estará sujeito a verificação pela Corregedoria e órgãos fiscalizadores.

Itapuranga-GO, _____ de _____ de 2026.

_____

Assinatura do Colaborador

_____

Talitha Durães Coelho Amorim
Tabeliã Titular

ANEXO I - CLASSIFICAÇÃO E CONTROLES PARA DOCUMENTOS E DADOS ELETRÔNICOS

Categoria	Definição	Exemplos	Controles Específicos (Conforme Provimento 213/2026 e LGPD)
Atos e Registros Eletrônicos Assinados	Documentos digitais que constituem o instrumento público ou registro formal, assinados com certificado ICP-Brasil.	Escrituras, atas notariais, protestos, registros de contratos marítimos.	- Assinatura Digital ICP-Brasil Obrigatória (Art. 6º) - Garantia de Irretratabilidade e Integridade (Art. 4º) - Cópia de segurança (backup) automatizada

Categoria	Definição	Exemplos	Controles Específicos (Conforme Provimento 213/2026 e LGPD)
			com retenção off-site - Logs de auditoria detalhados com identificação individualizada - Testes periódicos de restauração (no mínimo semestrais)
Dados Pessoais para Análise do Ato	Informações coletadas de clientes necessárias para a formação e validade do ato, incluindo dados sensíveis quando indispensáveis.	CPF, RG, endereço, filiação, dados patrimoniais, dados sensíveis (quando indispensável).	- Coleta limitada ao necessário para o ato (princípio da minimização) - Acesso restrito por usuário nominal e senha individual - Autenticação multifator (MFA) para acesso a funções críticas - Criptografia durante o armazenamento e trânsito (dados em repouso e em trânsito) - Registro de consentimento quando aplicável (dados

Categoria	Definição	Exemplos	Controles Específicos (Conforme Provimento 213/2026 e LGPD)
			sensíveis) - Retenção conforme tabela de temporalidade e eliminação segura.
Dados para Interoperabilidade	Informações transmitidas para sistemas nacionais, estaduais e órgãos de fiscalização.	Comunicações ao CENSEC, CESDI, RCTO, CBF, etc.	- Utilização de canais seguros e homologados - Observância dos padrões técnicos do CNJ e da Corregedoria - Registro em log das transmissões realizadas - Conformidade com os prazos e formatos exigidos
Documentos Internos e de Trabalho	Rascunhos, comunicações internas, manuais, minutas em elaboração.	Minutas não assinadas, e-mails internos, manuais de procedimento, rascunhos de atos.	- Acesso autenticado e restrito ao necessário - Eliminação segura após cumprir sua finalidade (destruição que impeça recuperação) - Não compartilhamento em canais não corporativos.

Categoria	Definição	Exemplos	Controles Específicos (Conforme Provimento 213/2026 e LGPD)
Logs e Trilhas de Auditoria	Registros de acesso e ações realizadas nos sistemas eletrônicos.	Histórico de acesso de usuários, alterações, consultas, transmissões.	- Retenção mínima de 5 anos ou conforme legislação específica - Inviolabilidade dos registros (imutabilidade) - Acesso restrito à administração e à fiscalização autorizada - Possibilidade de rastreabilidade completa de ações individuais.

ANEXO II - MATRIZ DE RESPONSABILIDADES (Alinhada ao Provimento 213/2026)

Função	Responsabilidades Principais em Segurança da Informação
Titular (Tabeliã)	- Responsável final pela segurança, integridade e disponibilidade dos atos e sistemas (Art. 5º) - Assinar digitalmente os atos com seu certificado ICP-Brasil - Autorizar, supervisionar e revisar periodicamente os níveis de acesso da equipe - Garantir os recursos necessários para a implementação

Função	Responsabilidades Principais em Segurança da Informação
	desta política - Comunicar incidentes à Corregedoria em até 72h - Designar formalmente o Encarregado (DPO)
DPO (Encarregado)	- Atuar como canal de comunicação com titulares, ANPD e Corregedoria - Supervisionar o cumprimento desta política e da LGPD - Gerenciar a resposta a incidentes de segurança e manter registros - Orientar a equipe sobre boas práticas de proteção de dados - Assegurar a realização de treinamentos periódicos
Notários e Escreventes	- Utilizar credenciais de acesso individuais e intransferíveis (Art. 5º) - Zelar pela confidencialidade de suas senhas e ativar MFA quando disponível - Bloquear a estação de trabalho sempre que se ausentar - Coletar apenas os dados estritamente necessários para o ato - Verificar a autenticidade dos documentos apresentados pelos clientes - Reportar imediatamente qualquer suspeita de incidente ao DPO e à Tabeliã
Equipe de TI (STI Soluções Tecnológicas)	- Implementar e manter os controles técnicos (backup, firewalls, antivírus, MFA) - Garantir a operação dos sistemas homologados e sua

Função	Responsabilidades Principais em Segurança da Informação
	interoperabilidade - Realizar os testes periódicos de restauração de backup (no mínimo semestrais) - Manter os logs de auditoria dos sistemas com integridade e retenção adequada - Monitorar continuamente servidores e redes (a cada 10 minutos) - Apoiar na resposta a incidentes e na comunicação técnica à Corregedoria
Prestadores de Serviço Terceirizados	- Assinar Termo de Conformidade com a Política de Segurança - Seguir as diretrizes de acesso e uso aceitável da serventia - Comunicar qualquer irregularidade identificada - Preservar sigilo sobre informações acessadas

---

ANEXO III - PROCEDIMENTOS PARA GARANTIR A IRRETRATABILIDADE

O cartório adota os seguintes procedimentos para garantir a irretratabilidade e a integridade do ato eletrônico:

1. **Assinatura com Certificado Válido:** Todo ato notarial ou registral será assinado digitalmente pela Tabeliã titular ou escrevente autorizado utilizando certificado digital ICP-Brasil do tipo A3, válido e dentro do período de vigência.

2. **Registro em Base Dedicada e Imutável:** Uma vez assinado, o ato é registrado em base de dados específica com mecanismos que impedem a alteração do seu conteúdo após a conclusão (WORM - Write Once, Read Many).

3. **Preservação do Hash e Metadados:** Os metadados e o hash digital (assinatura hash) do documento no momento de sua assinatura são preservados para permitir a verificação futura de sua integridade.

4. **Logs de Criação e Alteração:** Registro detalhado em log da data, hora, usuário e ação realizada, com impossibilidade de alteração ou exclusão dos registros.

5. **Backups com Verificação de Integridade:** Realização de backups diários com armazenamento off-site e testes periódicos de restauração que incluem a verificação da integridade dos arquivos (hash).

6. **Emissão de Cópias Autenticadas com Verificação:** As cópias e certidões fornecidas serão geradas a partir do original digital assinado e conterão mecanismos de verificação de autenticidade (ex: QR Code, código de verificação), permitindo que qualquer alteração no conteúdo da cópia seja detectada.

7. **Procedimento de Validação de Integridade:** Sempre que houver dúvida sobre a autenticidade de um documento, será realizado procedimento de validação comparando o hash do documento atual com o hash original armazenado.

8. **Certificação Temporal (Time Stamping):** Para atos que exijam prova temporal, será utilizado serviço de certificação de tempo (carimbo do tempo) conforme ICP-Brasil.
