Política de Privacidade

1. OBJETIVO

Esta Política estabelece as orientações gerais para a proteção de dados pessoais dentro do ambiente corporativo do controlador **TABELIONATO DE NOTAS E DE PROTESTO DE TITULOS E TABELIONATO E OFICIALATO DE REGISTRO DE CONTRATOS MARITIMOS**, inscrito no CNPJ sob o nº**55.807.183/0001-43,** CNS **150466**, doravante aqui denominado "**CONTROLADOR**", quando da execução de suas operações de coleta, manuseio, compartilhamento, armazenamento e eliminação de informações que podem estar relacionadas a pessoas físicas identificadas e/ou identificáveis ("Dados Pessoais"), com vistas a:

- estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas;
- proteger os direitos dos integrantes, clientes, fornecedores e parceiros contra os riscos de violações de Dados Pessoais;
- ser transparente com relação aos procedimentos do **CONTROLADOR** no Tratamento de Dados Pessoais; e
- promover a conscientização em toda o **CONTROLADOR** em relação à proteção de Dados Pessoais e questões de privacidade.

2. PUBLICO-ALVO

Essa política se aplica a todos os colaboradores, clientes, fornecedores e parceiros residentes no território brasileiro ou no exterior desde que possuam relacionamento com o **CONTROLADOR.**

Qualquer legislação aplicável às diferentes regiões, nas quais a companhia atua, devem prevalecer caso estejam ou venham estar em conflito com esta Política.

3. DEFINIÇÕES

Seguem abaixo as definições dos termos utilizados nesta Política.

Anonimização	Processo e técnica por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Dado anonimizado não é considerado Dado Pessoal.
Controlador	Pessoa jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais
Dado Pessoal	Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural

Dado Pessoal Sensível	Todo Dado Pessoal que pode gerar qualquer tipo de discriminação, como por exemplo os dados 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.
DPO / Encarregado de Proteção de Dados	O indivíduo designado como encarregado formal/oficial de proteção de dados, conforme previsto nas leis de proteção de dados, tais como GDPR e LGPD, para um determinado território. O DPO pode ser um integrante ou uma pessoa terceirizada.
LGPD	Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador.
Segurança da Informação – SI	Área responsável por proteger a integridade, disponibilidade e confidencialidade dos sistemas de TI e deve implementar as medidas adequadas para alcançar este objetivo, sendo o apoio técnico do Líder de Privacidade Corporativo e responsável pelas questões relacionadas às medidas técnicas e administrativas.
Titular de Dados	Pessoa natural singular identificada ou identificável a quem se refere um Dado Pessoal específico.
Tratamento de Dados Pessoais	Qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

4. PRINCÍPIOS DE PROTEÇÃO DE DADOS

A instituição determina que todos os dados utilizados no processamento devem estar em conformidade com a LGPD.

O artigo 7º da LGPD prevê que o tratamento de dados pessoais poderá ser realizado nas seguintes hipóteses:

1. mediante o fornecimento de consentimento pelo titular;
2. para o cumprimento de obrigação legal ou regulatória pelo controlador;
3. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
4. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
5. para a proteção da vida ou da incolumidade física do titular ou de terceiros;
6. quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
7. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Observa-se, por fim, que o processamento deve garantir uma adequada segurança dos dados pessoais, incluindo a contramedida de processamento não autorizado ou ilegal, perda acidental, destruição ou danos, deve sempre utilizar técnicas apropriadas ou as medidas organizacionais.

5. DIRETRIZES

A Gestão dos Dados, conforme esta Política, é de responsabilidade de todos os colaboradores, prestadores e coligadas, nos limites das atribuições de cada área envolvida.

A Gestão se dará, conforme atribuições descritas no item “principais papéis e responsabilidades desta Política, nos Ambientes declarados Informacionais, Analíticos e entre outros”, a partir da execução de processos e monitoramentos descritos abaixo:

1. Esta política deve ser revista no mínimo anualmente;
2. Em qualquer observação ou constatação de não aderência a essa política, deve ser informado imediatamente ao DPO ou Encarregado de Proteção de Dados como assim definido pela respectiva Lei Geral de Proteção de Dados; e
3. Observar na Lei Geral de Proteção de Dados a Sanção II – Das Boas Práticas e da Governança.

6. PRINCIPAIS PAPÉIS E ATRIBUIÇÕES

O DPO ou Encarregado de Proteção de Dados, como assim definido pela respectiva Lei Geral de Proteção de Dados é pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Além do mais, é o responsável pela gestão conjunta de política e procedimentos, relativas à Gestão de Dados.

7, POLÍTICA

O processamento deve ser transparente, lícito, justo e deverá manter registros nos sistemas envolvidos, e os acessos aos dados devem ser:

1. Revisados anualmente;
2. Os titulares de dados têm o direito de acesso aos seus dados pessoais e quaisquer solicitações feitas para a empresa e sem demora, conforme Art. 20 da LGPD; e
3. Devem ser providos de forma clara e transparente os dados dos titulares, conforme § 1º.

7.1 PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

Esta seção descreve os princípios que devem ser observados na coleta, manuseio, armazenamento, divulgação e Tratamento de “Dados Pessoais” pela empresa para atender aos padrões de proteção de dados no âmbito corporativo e estar em conformidade com a legislação e regulamentação aplicáveis nos respectivos países onde tiver operação ou atividade comercial.

7.2 LEGALIDADE, TRANSPARÊNCIA E NÂO DISCRIMINAÇÃO

A companhia trata os Dados Pessoais de forma justa, transparente e em conformidade com legislação e regulamentação aplicáveis.

O **CONTROLADOR** somente trata Dados Pessoais quando o propósito/finalidade do Tratamento se enquadra em uma das hipóteses legais permitidas, sendo certo que os Titulares de Dados devem ser informados sobre a razão e a forma pela qual seus Dados Pessoais estão sendo tratados antes ou durante a coleta:

- necessidade para a execução de um contrato do qual o titular dos dados é parte;
- exigência decorrente de lei ou regulamento ao qual a companhia está sujeita;

- interesse legítimo pelo Tratamento, hipótese na qual tal interesse legítimo será comunicado previamente; e
- necessidade de prover ao titular dos dados o exercício regular de direito em processo judicial, administrativo ou arbitral.

Quando o Tratamento de Dados Pessoais não se enquadrarem nas hipóteses acima, a companhia deve obter o consentimento dos titulares dos dados para o tratamento de seus dados pessoais, e assegurar que este consentimento seja obtido de forma específica, livre, inequívoca informada. A companhia deve coletar, armazenar e gerenciar todas as respostas de Consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser fornecida quando necessário.

Da mesma forma, o Titular de Dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento com a mesma facilidade que lhe foi fornecido.

Em algumas circunstâncias a companhia também pode ser obrigada a tratar Dados Pessoais Sensíveis, envolvendo, mas não limitado a:

- dados relacionados à saúde ou à vida sexual;
- dados genéticos ou biométricos vinculados a uma pessoa física;
- dados sobre orientação sexual;
- dados sobre condenações ou ofensas criminais;
- dados que evidenciem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas; e
- dados referentes à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O Tratamento de Dados Pessoais Sensíveis é proibido, exceto nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais Dados Pessoais:

- quando for necessário para o cumprimento de obrigação legal ou regulatória;
- quando for necessário para o exercício regular de direitos como, por exemplo, defesa ou proposição de ações judiciais ou administrativas ou arbitrais;
- quando for necessário para o cumprimento de obrigações e o exercício de direitos em matéria de emprego, previdência social e proteção social;
- para proteção à vida ou à incolumidade física do Titular do Dado incluindo dados médicos com fins preventivos, ocupacional;
- para fins de promoção ou manutenção de igualdade de oportunidades entre pessoas de origem racial ou étnica diferente,
- quando o Titular dos Dados tiver dado o seu Consentimento explícito, de acordo com a legislação e regulamentação aplicáveis; e
- quando o Tratamento for relativo a condenações penais e infrações ou a medidas de proteção relacionadas será efetuado sob o controle da autoridade pública ou quando o Tratamento for autorizado pela legislação da União ou de um Estado-Membro que preveja as salvaguardas adequadas para os direitos e liberdades dos Titulares de Dados Pessoais.

7.3 LIMITAÇÃO E ADEQUAÇÃO DA FINALIDADE

O Tratamento de Dados Pessoais deve ser realizado de maneira compatível com a finalidade original para a qual os Dados Pessoais foram coletados, não podendo ser coletados com um propósito e utilizados para outro. Quaisquer outras finalidades devem ser compatíveis com a razão original para qual os Dados Pessoais foram coletados.

O acesso às informações pessoais coletadas é extremamente restrito às pessoas autorizadas e envolvidas no processamento para a qual a finalidade coletada.

7.4 NECESSIDADE (MINIMIZAÇÃO DOS DADOS)

O **CONTROLADOR** somente pode tratar Dados Pessoais na medida em que seja necessário para atingir um propósito específico, este é o princípio da minimização de dados. O compartilhamento de Dados Pessoais com outra área ou outra empresa deve considerar este princípio, só podendo ser compartilhados quando tenham um amparo legal adequado.

7.5 DADOS COLETADOS PARA CONTRATAÇÃO

1. O **CONTROLADOR** somente coletará os dados pessoais necessários dos candidatos, para a finalidade de contratação, quando este partir de anúncios de vagas disponibilizados, podendo assim se utilizar das hipóteses de tratamento, procedimentos preliminares a execução de contrato e/ou legítimo interesse, em seu artigo 7.
2. Todos os currículos entregues fisicamente ou eletronicamente por parte do titular, sem que haja por parte do **CONTROLADOR** a disponibilização de vagas, estará justificado na hipótese de tratamento como consentimento, definido em artigo 7, inciso I.
3. Todos os currículos não aprovados em processo seletivo, serão preservados por tempo indeterminado para composição de banco de talento, para futuras entrevistas de vagas de emprego. O **CONTROLADOR** se compromete em adotar todas as medidas segurança suficiente para garantir que pessoas não autorizadas não tenham acesso aos respectivos dados.
4. Todos os currículos selecionados a descarte, serão descartados de forma segura conforme definido na política de descarte, obedecendo sua tabela de temporalidade.

7.6 DADOS TRATADOS PARA FINALIDADES FINANCEIRAS

O **CONTROLADOR**, trata os dados de seus clientes para execução contratual na emissão cobrança bancária referente aos serviços contratados e prestados.

7.7 EXATIDÃO (QUALIDADE DOS DADOS)

O **CONTROLADOR** adota medidas razoáveis para assegurar que quaisquer dados pessoais em sua posse sejam mantidos precisos, atualizados em relação às finalidades para as quais foram coletados, sendo certo que deve ser possibilitado ao Titular do Dado Pessoal a possibilidade de se requerer a exclusão ou correção de dados imprecisos ou desatualizados.

7.8 OBRIGAÇÃO LEGAL REGULARÓRIA

O **CONTROLADOR** possui como base principal o cumprimento de obrigação legal ou regulatória conforme descrito na lei 8.935/94.

O **CONTROLADOR** por obrigação, necessita compartilhar seus dados com: COAF, RCTO, CESDI, CEP, CENSEC e CNISP[1].

7.9 RETENÇÃO E LIMITAÇÃO DO ARMAZENAMENTO DE DADOS

Todos os dados coletados, assim como também os documentos, serão armazenados por tempo necessário para o cumprimento da finalidade para a qual foram coletados, salvo quando necessário para o cumprimento de obrigatoriedade regulatória.

Cada categoria de documento possui seu prazo definido na tabela de temporalidade.

7.10 INTEGRIDADE E CONFIDENCIALIDADE (LIVRE ACESSO, PREVENÇÃO E SEGURANÇA)

O **CONTROLADOR** adota medidas técnicas e administrativas necessárias e apropriadas para proteger os Dados Pessoais contra o Tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O Tratamento de Dados Pessoais também deve garantir a devida confidencialidade.

7.11 RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

O **CONTROLADOR** é responsável e deve demonstrar o cumprimento desta Política, assegurando a implementação de diversas medidas que incluem, mas não se limitam a:

- garantia de que os Titulares dos Dados Pessoais possam exercer os seus direitos conforme descritos na Seção 5.5 deste Documento;
- registro de Dados Pessoais, incluindo: o registro de atividades de Tratamento de Dados Pessoais, com a descrição dos propósitos/finalidades desse Tratamento, os destinatários do compartilhamento dos
- informações sobre Dados Pessoais e os prazos pelos quais O **CONTROLADOR** deve retê-los;
- registro de incidentes de Dados Pessoais e violações de Dados Pessoais;
- garantia de que os Terceiros que sejam Processadores de Dados Pessoais também estejam agindo de acordo com esta Política e com a legislação e regulamentação aplicáveis;
- garantia de que O **CONTROLADOR**, quando requerido, registre junto à Autoridade Supervisora aplicável um Encarregado de Dados ou DPO; e
- garantia de que O **CONTROLADOR** esteja cumprindo todas as exigências e solicitações de qualquer Autoridade de Supervisão à qual esteja sujeita.

8. INFORMAÇÕES COMPLEMENTARES

Todos os dados pessoais processados, deve ser feito em uma das seguintes análises de bases legais: autorização, contrato, obrigação legal, de interesses vitais, público ou interesses legítimos:

1. A áreas devem observar a adequação legal, e realizar o registro do tratamento do dado;
2. O consentimento deve ser armazenado no mesmo sistema ou em algum outro que possa ser de fácil acesso, conforme - Art. 5º - XII e Art. 8º - § 1º; e
3. Em qualquer momento os titulares dos dados podem revogar os acessos, mediante as bases legais ou outras que subsidie as demais atividades, conforme Art. 8º - § 2º e Art. 18.

9. MINIMIZAÇÃO DE DADOS

A companhia aplica o princípio da necessidade, conforme Art. 6 III, em todas suas atividades de tratamento de dados, garantindo assim que somente os dados necessários sejam coletados para a execução de suas finalidades.

10. REGRAS DETERMINANTES

A companhia tomará medidas razoáveis para garantir que os dados dos titulares coletados estejam sempre atrelados à necessidade e apoiados nas bases legais permissivas para tanto, conforme Artigos 7º, 8º 11 e 14 de LGPD.

11. ARMAZENAMENTO OU DELEÇÃO

Para garantir que os dados pessoais não serão conservados durante mais tempo do que o necessário, este armazenamento deve estar apoiado nas bases legais.

O armazenamento dos dados pessoais pode decorrer pela permanência do contrato em vigor e deve estar explícita a deleção após o término do interesse entre as partes.

Este item observa a Lei Geral de Proteção de dados Seção IV da respectiva lei.

12. SEGURANÇA

1. Dever dos funcionários de garantir que os dados pessoais são armazenados de forma segura, utilizando-se medidas protetivas, bem como:
2. O acesso a dados pessoais deverá ser limitado as pessoas que precisam de acesso e não é autorizado o compartilhamento das informações;
3. Quando dados pessoais são apagados, isso deve ser feito com segurança, de tal forma que os dados se tornem irrecuperáveis; e
4. O backup e soluções de recuperação de desastres deve seguir o procedimento “backup para recuperação”.
5. O **CONTROLADOR** está comprometida com a implementação dos padrões de Segurança da Informação e com a proteção de Dados Pessoais com vistas a garantir o direito fundamental do indivíduo à autodeterminação da informação.
6. A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não repúdio são objetivos a serem perseguidos para a segurança dos Dados Pessoais.
7. Todos os Integrantes com acesso a dados pessoais estão obrigados aos deveres de confidencialidade dos Dados Pessoais mediante a anuência no Código de Conduta do **CONTROLADOR** e periodicamente quando necessário.
8. Ao implementar novos processos, procedimentos ou sistemas que envolvam o Tratamento de Dados Pessoais, O **CONTROLADOR** deve adotar medidas para garantir que as regras de Privacidade e Proteção de Dados sejam adotadas desde a fase de concepção até o lançamento/implantação destes projetos.
9. Cada Sociedade/Filial Controlada do **CONTROLADOR** é o Controlador dos Dados Pessoais em sua respectiva região ou empresa, sendo necessária a nomeação de um responsável por garantir que os Dados Pessoais estejam sendo tratados de forma correta e de acordo com a legislação e regulamentação aplicáveis naquela região. Em determinadas circunstâncias, uma Filial Controlada do **CONTROLADOR** pode atuar como Processadora de outra. Nestes casos, a Processadora é obrigada a seguir a orientação de quem está atuando como Controladora.
10. Quando os Dados Pessoais forem tratados em países diferentes de onde foram coletados, a legislação e regulamentação aplicáveis à transferência internacional de dados de cada país devem ser observadas. O **CONTROLADOR** deve garantir a existência e atualização de contratos de transferência internacional de Dados Pessoais.

13. DIREITOS DOS TITULARES DE DADOS PESSOAIS

O **CONTROLADOR** está comprometida com os direitos dos Titulares de Dados Pessoais, os quais incluem:

- a informação, no momento em que os Dados Pessoais são fornecidos, sobre como seus Dados Pessoais serão tratados;
- a informação sobre o Tratamento de seus Dados Pessoais e o acesso aos Dados Pessoais que O **CONTROLADOR** detenha sobre eles;
- a correção de seus Dados Pessoais se estiverem imprecisos, incorretos ou incompletos;
- a exclusão, bloqueio e/ou anonimização de seus Dados Pessoais em determinadas circunstâncias (“direito de ser esquecido”). Isso pode incluir, mas não se limita a, circunstâncias em que não é mais necessário que O **CONTROLADOR** retenha seus Dados Pessoais para os propósitos para os quais foram coletados;
- a restrição do Tratamento de seus Dados Pessoais em determinadas circunstâncias;
- opor-se ao Tratamento, se o Tratamento for baseado em legítimo interesse
- a retirar o Consentimento a qualquer momento, se o Tratamento dos Dados Pessoais se basear no Consentimento do indivíduo para um propósito específico;
- a portabilidade dos Dados Pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa em determinadas circunstâncias;
- a revisão das decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais; e
- a apresentação de queixa à **CONTROLADOR** ou à Autoridade de Proteção de Dados aplicável, se o Titular dos Dados Pessoais tiver motivos para supor que qualquer um de seus direitos de proteção de Dados Pessoais tenha sido violado.

14. PRESTADORA DE SERVIÇOS TERCEIRIZADOS

Os prestadores de serviços terceirizados que tratem Dados Pessoais sob as instruções do **CONTROLADOR**, estão sujeitos às obrigações impostas aos processadores de acordo com a legislação e regulamentação de proteção de Dados Pessoais aplicáveis. O **CONTROLADOR** deve assegurar que no contrato de prestação de serviço sejam contempladas as cláusulas de privacidade que exijam que o Processador de Dados terceirizado implemente medidas de segurança, bem como controles técnicos e administrativos apropriados para garantir a confidencialidade e segurança dos Dados Pessoais e especifiquem que o Processador está autorizado a tratar Dados Pessoais apenas quando seja formalmente solicitado pelo **CONTROLADOR**.

Nos casos em que o prestador de serviços estiver localizado fora do país em que o Dado Pessoal foi coletado, as cláusulas contratuais padrão deve ser incluídas no contrato de proteção de Dados Pessoais como um Anexo para garantir que as devidas salvaguardas exigidas pela legislação e regulamentação aplicáveis de proteção de Dados Pessoais.

15. VIOLAÇÃO

No caso de violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais, a companhia deverá prontamente avaliar o risco para os direitos e liberdades das pessoas e, se apropriado, informar essa violação à autoridade competente.

Todos os incidentes e potenciais violações de dados devem ser reportadas ao Líder de Privacidade Corporativo e/ou DPO/Encarregado de Proteção de Dados Pessoais.

O Encarregado de Proteção de Dados deverá avalizar o fato ocorrido, afim de identificar a necessidade de reportar à ANPD e aos titulares de dados que tiveram seus dados pessoais envolvidos neste evento.

Todos os Integrantes devem estar cientes de sua responsabilidade pessoal de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de Dados Pessoais assim que as identificarem.

No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva. Violações de Dados incluem, mas não se limitam a qualquer perda, exclusão, roubo ou acesso não autorizado de Dados Pessoais controlados ou tratados pelo **CONTROLADOR.**

Este item da política observa a Lei Geral de Proteção de Dados Seção II – Da Responsabilidade.

16. AUDITORIAS DE PROTEÇÃO DE DADOS

O **CONTROLADOR** deve garantir que existam revisões periódicas a fim de confirmar que as iniciativas de Privacidade, seu sistema, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de Dados Pessoais são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

17. NORMAS EXTERNAS RELACIONADAS E OUTRAS REGÊNCIAS DE MERCADO

- **LEI Nº 12.965 - Marco Civil:** Tem como objetivo precípuo oferecer segurança jurídica aos usuários da rede, sejam eles internautas, empresas, provedores e Administração Pública.
- **Resolução nº 4.658 BACEN**: Trata sobre segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Lei 105/01 - Leio de sigilo Bancário.
- **LGPD** – Lei Geral de Proteção de Dados – 13.709/2018.
- **27001 –** Security Foundation.
- **NIST –** National Institute of Standards and Technology.

Data: 18/05/2026

ELABORADO POR:

Encarregado de Proteção de Dados

CNPJ: 20.705.613/0001-31

Representada por: Wellington Rodrigues da Silva

Data: / /

Assinado digitalmente por:

Por: INOVALGPD CONSULTORIA E TREINAMENTOS LTDA
Encarregado de Proteção de Dados: Wellington Rodrigues da Silva
CNPJ: 20.705.613/0001-31
Em: Terça-feira, 25 de Agosto de 2026, 13:01
Doc: ADM-20260518-005 v1 |SHA256: 960eb01d7764e9083adb2248009674405539d517406cd471e63a21242c1a013f

InovaLGPD Consultoria e Treinamentos LTDA

APROVADO POR:

MARILIA DE ABREU OLIVEIRA:70112865194

Assinado de forma digital por MARILIA DE ABREU OLIVEIRA:70112865194
Dados: 2026.08.25 13:15:00 -03'00'

Oficial Titular

TABELIONATO DE NOTAS E DE PROTESTO DE TITULOS E TABELIONATO E OFICIALATO DE REGISTRO DE CONTRATOS MARITIMOS

CPF/CNPJ: 55.807.183/0001-43

CNS/CNJ: 150466

[1]Registro Central de Testamentos Online (RCTO); Central de Escrituras de Separações, Divórcios e Inventários (CESDI); Central de Escrituras e Procurações (CEP); e Central Nacional de Sinal Público (CNISP)