LGPD

HISTÓRICO DAS REVISÕES

Este manual encontra-se disponível na Intranet da serventia, no sistema SGT, e no site do cartório. O Manual de LGPD é disponibilizado a todas as partes interessadas e poderá ser alterado a qualquer tempo a critério da liderança do cartório, de acordo com a atualização das normas e leis. Todas as alterações entram em vigor imediatamente após a publicação.

Revisão Nº	Item	Natureza da Alteração	Data	Autorizado por
01		Revisão geral	10/09/2025	Vivianne
02		Revisão geral, sem alterações	15/04/2026	Vivianne

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1.1. INTRODUÇÃO

O 2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS (o "Cartório") tem como missão prestar os serviços relativos a suas atribuições com qualidade, agilidade e eficiência, prezando pelo respeito, a satisfação e a confiabilidade da sociedade.

O Cartório entende que as informações e os dados são bens essenciais para suas atividades, tanto no que se refere à sua própria execução quanto no que se refere à qualidade e eficiência em seu fornecimento.

O Cartório compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, cuja vulnerabilidade a fatores externos e internos podem comprometer a segurança das informações e a privacidade de dados pessoais, sejam de clientes ou colaboradores.

Dessa forma, o Cartório estabelece sua Política de Segurança da Informação (a "PSI") como parte integrante do seu sistema de gestão, alinhada às diretrizes legais e administrativas, às boas práticas e às normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações do Cartório ou sob sua responsabilidade.

1.2. OBJETIVOS

Declarar formalmente as diretrizes do 2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS DE GOIÂNIA que visam à proteção dos ativos de informação e privacidade dos dados pessoais com eficiência e eficácia, de modo seguro, garantindo a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade, assim como dos Ativos de Tecnologia de Informação e Comunicação que as sustentam, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios de acordo com a atividade notarial e registral exercida.

Estabelecer as competências, responsabilidades e limites de atuação dos colaboradores do Cartório em relação à segurança da informação e da privacidade, reforçando a cultura de segurança e priorizando as ações necessárias conforme suas atividades.

1.3. APLICAÇÃO

Esta Política de Segurança da Informação é um documento de aplicabilidade imediata, plena e indistinta a todos os empregados, estagiários, menores aprendizes, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as informações e os ativos do Cartório ou sob sua responsabilidade.

1.4. PRINCÍPIOS

Preservar e proteger a informação em todo o seu ciclo, contida em qualquer meio, suporte ou formato, de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenir e reduzir impactos gerados por incidentes de segurança, assegurando a confidencialidade, integridade, disponibilidade, autenticidade e legalidade no desenvolvimento das atividades profissionais.

Estabelecer e definir as atribuições e responsabilidades do Comitê de Segurança da informação e privacidade visando alcançar os objetivos e estabelecer os controles definidos pelo Cartório.

Assegurar que a Tecnologia da Informação realize a gestão e a segurança dos ativos de propriedade do2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS DE GOIÂNIA ou dos que estão sob sua responsabilidade.

Promover a constante capacitação e reforçar a conscientização direcionada ao desenvolvimento e manutenção das habilidades e aperfeiçoamento dos colaboradores sobre tecnologia e segurança da informação.

Cumprir a legislação vigente e demais instrumentos e normativas relacionados às suas atribuições no que diz respeito à segurança da informação e aos objetivos institucionais, morais e éticos do Cartório.

1.5. DIRETRIZES GERAIS

Integração: Esta PSI e seus documentos complementares fazem parte integrante do Controle de Fluxo previsto no art. 1337, II, j do Código de Normas e Procedimentos do Foro Extrajudicial.

Interpretação: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização, devendo ser levada em consideração a análise de risco e a necessidade operacional à época de sua solicitação.

Publicidade: Esta PSI e seus documentos complementares devem ser divulgados aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com o 2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS ou que, direta ou indiretamente, são impactados.

Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade e direito de uso exclusivo do 2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS e devem ser empregados unicamente para fins profissionais.

Propriedade Intelectual: É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, do 2º TABELIONATO DE PROTESTO DE TÍTULOS E DOCUMENTOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS em qualquer forma ou mídia, inclusive na Internet e nas mídias sociais, sem a prévia e formal autorização para tanto, até mesmo no âmbito acadêmico.

Classificação da Informação: Os colaboradores devem utilizar apenas os recursos disponibilizados

pelo Cartório para classificar a informação e aplicar os respectivos controles estabelecidos em documento específico, em todo o ciclo de vida da informação, ou seja, desde a sua recepção ou produção até o seu descarte.

Sigilo: É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade do Cartório por seus colaboradores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja classificada como "pública".

Uso dos Ativos: Os ativos de propriedade do Cartório devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

O colaborador deve utilizar apenas ativos previamente homologados e autorizados pelo TI, sejam eles onerosos, gratuitos, livres ou licenciados.

Manutenção dos Ativos: Todos os ativos em uso no ambiente corporativo do Cartório devem atender as recomendações de seus fabricantes ou desenvolvedores no que diz respeito à manutenção e correções de falhas técnicas de segurança.

Mobilidade: Os ativos que permitem mais mobilidade ao colaborador devem ser utilizados somente quando fornecidos ou autorizados pelo Cartório. Além disso, devem estar diretamente relacionados a uma justificativa do negócio, com motivo estritamente profissional, no âmbito das atribuições do colaborador.

Ativos Particulares: O uso de ativos particulares na execução de qualquer atividade profissional ou na interação com os ambientes físicos ou lógicos ou com as informações do Cartório deve ocorrer somente após solicitação formal e fundamentada do colaborador solicitante e autorização expressa do TI.

Repositórios digitais: É vedado aos colaboradores o uso de repositórios digitais não homologados pela TI para armazenar ou publicar informações de propriedade ou sob a responsabilidade do Cartório, salvo nos casos em que a informação esteja classificada como pública.

Softwares de comunicação instantânea: É vedado aos colaboradores a instalação e o uso de softwares de comunicação instantânea não homologados pela TI nos ativos do Cartório.

Mídias Sociais: A participação do colaborador nas mídias sociais por meio dos ativos do Cartório deve ser realizada de acordo com controles estabelecidos em documento específico e estar relacionada às atividades profissionais.

O colaborador é responsável por sua conduta no uso das mídias sociais. Por isso, cuidados devem ser tomados em relação ao excesso de exposição (rotinas, trajetos, intimidade, etc), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.

Controle de acesso: O Cartório controla o acesso físico e lógico às suas dependências e aos seus ativos. Desse modo, cada colaborador deve possuir um login e senha de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

O colaborador é responsável pelo uso e sigilo de suas credenciais de acesso, não sendo permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de logins e senha de terceiros, responsabilizando-se diretamente pela conduta ou/e dano causado.

Ambientes Lógicos: Os sistemas e processos que suportam os ativos do Cartório devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.

Ambientes Físicos: O Cartório deve implementar controles de identificação e registro de acesso em suas dependências para assegurar o acesso somente de colaboradores autorizados.

Áudio, Vídeos e Fotos: É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências do Cartório por seus colaboradores sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico ou uso nas mídias sociais.

Contratação, Terceirização ou Prestação de Serviços: Os relacionamentos e contratações, inclusive de colaboradores, em que ocorra o compartilhamento de informações do Cartório ou a concessão de qualquer tipo de acesso aos seus ambientes e ativos, devem ser precedidos por termos de

confidencialidade e cláusulas contratuais relacionadas à segurança da informação e privacidade.

Desenvolvimento e aquisição de software: O desenvolvimento interno e/ou externo de softwares, assim como a aquisição de softwares e produtos no mercado, devem possuir requisitos de segurança para garantir informações confiáveis, íntegras, autênticas e oportunas.

Documentação: O Cartório deve possuir documentação adequada e suficiente referente a recuperação em situações de contingência de seus sistemas e processos que envolvam seus ativos.

Salvaguarda (*backup*): O Cartório deve definir e manter um processo de salvaguarda e restauração das informações e de seus ativos críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

Análise dos processos e ativos: O Cartório deve analisar, em intervalos regulares, seus processos e ativos, visando assegurar que estes estejam devidamente mapeados, inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança identificadas.

Monitoramento: O Cartório realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, ativos e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados e a proteção de seu patrimônio, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.

Inspeção dos Ativos: O Cartório, sempre que considerar necessário, pode auditar ou inspecionar os ativos que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os Ativos de propriedade de terceiros quando autorizada a entrada em suas dependências.

Gestão de Configuração e Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica do Cartório devem preservar os controles relacionados à disponibilidade, integridade, sigilo e autenticidade das informações.

Continuidade do Negócio: Os procedimentos de Gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de segurança da informação e privacidade estabelecidos para proteção dos ativos críticos.

Conformidade: O Cartório deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente.

Capacitação: O Cartório deve promover, junto aos seus colaboradores, a capacitação e a constante conscientização visando a disseminação da cultura da segurança da informação, proteção de dados e privacidade.

Investimentos: Os investimentos em segurança da informação e privacidade no Cartório devem ser estudados e deliberados conjuntamente com o CSI, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

Comitê de Segurança da Informação (CSI): O Cartório deve manter um Comitê de Segurança da Informação (CSI), cuja principal função está em assessorar a implementação das ações relacionadas à segurança da informação e da privacidade, além de avaliar os controles, violação de dados pessoais e incidentes relacionados.

Equipe de Resposta a Incidentes (ERI): De forma a agilizar a resposta, sob a estrutura do CSI haverá uma Equipe de Resposta a Incidentes em segurança da informação e privacidade, composta de 03 (três) integrantes sendo o encarregado, o responsável pelo TI e um dos tabeliães-substitutos, preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação.

Comunicação de Incidentes: O Cartório deve possuir um canal de comunicação divulgado aos seus colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação e privacidade, podendo fazer de modo formal ou com uso do recurso de denúncia anônima.

Alterações: As alterações desta PSI e de seus documentos complementares devem ser devidamente comunicadas aos seus colaboradores pelo Cartório.

Exceções: As exceções que ocorram de forma exclusiva e excepcional a essa PSI, devem ser formalizadas e fundamentadas pelo colaborador solicitante, e podem ser revogadas a qualquer tempo, por mera liberalidade do Cartório.

As medidas alternativas às previstas nesta PSI, realizadas de modo excepcional para mitigar riscos em ocasiões específicas e justificáveis, inclusive em situações emergenciais, devem ser formalizadas e fundamentadas pelo colaborador de forma imediata ou assim que possível ao CSI.

Dúvidas: Qualquer dúvida relativa a esta PSI deve ser encaminhada ao CSI por meio do e-mail csi@2prtd.com.br

1.6. INCIDENTES DE SEGURANÇA

Análise e Comunicação: Os incidentes de segurança da informação devem ser imediatamente analisados pela ERI e avaliados pelo CSI. Verificada a ocorrência de incidente com dados pessoais, o encarregado comunicará o controlador para que este promova a comunicação ao Corregedor Permanente na forma prevista no art. 1.340 do Código de Normas e Procedimentos do Foro Extrajudicial do Estado de Goiás.

Procedimento e Penalidades: Ao avaliar o caso, o CSI poderá instaurar e apurar as responsabilidades dos envolvidos em procedimento administrativo, visando aplicação de sanções cabíveis previstas em cláusulas contratuais, regimento interno e outros documentos normativos do Cartório além da legislação vigente.

Tentativa de Burla: A tentativa de burlar às diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação para todos os fins.

1.7. PAPÉIS E RESPONSABILIDADES

1.7.1. Comitê de Segurança da Informação e Privacidade (CSI)

Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação, privacidade e proteção de dados.

Garantir a disponibilidade dos recursos necessários para uma efetiva gestão de segurança da informação e privacidade.

Garantir que as atividades de segurança da informação, privacidade e proteção de dados, sejam executadas em conformidade com a PSI.

Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do Cartório.

1.7.2. Tecnologia da Informação (TI)

Conduzir a gestão e operação da segurança da informação, privacidade e proteção de dados, tendo como base esta política e demais resoluções do CSI.

Apoiar o CSI em suas deliberações.

Elaborar e propor ao CSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PSI.

Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas preventivas e corretivas pertinentes.

Tomar as ações cabíveis para se fazer cumprir os termos desta política.

Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

1.7.3. Encarregado

Gerenciar as informações geradas ou sob a responsabilidade da sua área durante todo o seu ciclo, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo Cartório.

Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área conforme normas, critérios e procedimentos adotados pelo Cartório.

Periodicamente revisar as referidas informações, ajustando a classificação e rotulagem das mesmas conforme necessário.

Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade.

Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo cartório.

Adotar as medidas cabíveis nos casos de incidência e segurança conforme art. 1.340 do Código de Normas e Procedimentos do Foro Extrajudicial.

Receber reclamações e sugestões e prestar informações aos usuários.

Atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

1.7.4. Recursos Humanos

Apoiar o CSI na elaboração de campanhas de conscientização e materiais de divulgação e alerta em segurança da informação e privacidade.

Estipular controles de segurança e proteção de dados especificamente relacionados aos processos

de contratação, desligamento (ou encerramento de prestação de serviços), modificação de atividades (incluindo a promoção) e afastamentos (incluindo férias e quaisquer licenças ou suspensões);

Comunicar à TI o desligamento dos colaboradores e término de contratações, para que os acessos destes sejam desativados.

Cabe ao RH divulgar internamente a PSI e demais documentos complementares e viabilizar, juntamente com o CSI, cursos, conferências, seminários, treinamentos e palestras sobre segurança e privacidade das informações.

Cabe ao RH colher assinatura dos operadores no documento "Termo de Ciência de Deveres, Responsabilidade e Requisitos", mediante orientação sobre os deveres, requisitos e responsabilidades na coleta, tratamento e compartilhamento de dados pessoais a que tiverem acesso.

Disponibilizar e realizar a gestão das credenciais individuais de acesso ao ambiente físico do Cartório.

1.8. GESTÃO DA POLÍTICA

A Política de Segurança da Informação é aprovada pelo Comitê de Segurança da Informação, em conjunto com o Titular do Cartório.

2. POLÍTICA DE PRIVACIDADE E DE PROTEÇÃO DE DADOS

2.1. INTRODUÇÃO

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados ou, simplesmente, "LGPD") regula o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e privacidade.

A lei coloca o cidadão na figura de titular de seus dados e, sob esse prisma, estabelece diretrizes importantes e obrigatórias para a coleta, o processamento e o armazenamento e exclusão de dados pessoais, tanto nos meios digitais quanto físicos.

Por meio deste Manual de Política de Privacidade e de Proteção de Dados (o "Manual" ou a "Política"), você tomará conhecimento das principais diretrizes, políticas, princípios, normas e compromissos do 2º TABELIONATO DE PROTESTO DE TÍTULOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS DE GOIÂNIA (o "Cartório" ou o "Controlador") relativos à privacidade e segurança das informações fornecidas pelos usuários. Tudo com o objetivo de esclarecer sobre os tipos de dados tratados, a finalidade desse tratamento e como o usuário poderá gerenciar seus dados pessoais.

O presente Manual está em conformidade com a Lei nº 13.709/2018, com a Lei nº 12.965/2014 (Marco Civil da Internet) e com o Código de Normas e Procedimentos do Foro Extrajudicial da Corregedoria-Geral da Justiça de Goiás. Seu conteúdo será revisado sempre que necessário para adequação às normas legais ou administrativas ou, ainda, em razão de alterações circunstanciais significativas, tais como inovações tecnológicas e boas práticas, se comprometendo o Cartório em manter uma versão atualizada deste documento publicamente acessível no site e no Cartório.

Caso o usuário tenha dúvidas sobre o tratamento dos seus dados, recomendamos entrar em contato com nosso DPO encarregado do atendimento ao titular de dados, através do endereço eletrônico encarregado@2prtd.com.br, conforme instruções no item 12 deste Manual.

A garantia da segurança jurídica é um dos nossos valores mais importantes e a proteção dos seus dados pessoais é uma prioridade para nós.

2.2. DEFINIÇÕES

A fim de facilitar sua leitura e familiarização com os termos utilizados na LGPD, empregados neste Manual ou mesmo encontrados em políticas de privacidade em geral, apresentamos algumas definições úteis sobre o tema:

- "Dado Pessoal": toda informação relacionada à pessoa natural identificada ou identificável, ou seja, qualquer informação que identifique ou possa identificar uma pessoa, tais como nomes, números de documento, endereços, etc.

- "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.

- "Titular de Dados Pessoais" ("Titular", "Usuário", "Você"): pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; titular de dados pessoais que acessa a plataforma do Cartório.
- "Plataforma": o *site* www.2prtd.com.br de titularidade do Cartório.
- "Tratamento de Dados Pessoais" ("Tratamento"): É toda a operação realizada com o dado pessoal, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, comunicação, transferência, difusão ou extração.
- "Controlador": pessoa natural ou jurídica, de direito público ou privado, que tem competência para tomar decisões referentes ao tratamento de dados pessoais.
- "Operador": pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- "Autoridade Nacional de Proteção de Dados" ("ANPD"): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.
- "Encarregado" ou "DPO" (*Data Protection Officer*): 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.
- "Consentimento": manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- "Eliminação": exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- "Terceiro": pessoa física ou jurídica, autoridade pública, agência ou organismo que não seja o titular dos dados, controlador, operador e pessoas que, sob a autoridade direta do controlador ou operador, estão autorizadas a tratar dados pessoais.
- "Segurança dos Dados": medidas técnicas e administrativas aptas a proteger a segurança dos dados no seu tratamento.
- "Cookies": arquivos salvos em seu computador, *tablet* ou telefone quando você visita um *site*. Usamos os cookies necessários para fazer o *site* funcionar da melhor forma possível e assim, oferecer serviços de qualidade. Alguns *cookies* são classificados como necessários e permitem a funcionalidade central, como segurança, gerenciamento de rede e acessibilidade. Esses *cookies* podem ser coletados e armazenados assim que você inicia sua navegação ou quando usa algum recurso que os requer.
- "Pixels': partes do código Java Script, instalados adicionados em aplicações, websites ou no corpo de um e-mail, com a finalidade de rastrear e coletar informações sobre as atividades dos usuários,

permitindo a identificação dos seus padrões de acesso, navegação, interesse e compras de produtos, para otimizar o direcionamento de conteúdo.

- "Web beacon": técnica que permite mapear quem está visitando uma determinada página da web, identificando o comportamento do usuário com diferentes sites ou servidores da web.
- "Ferramentas de analytics": ferramentas que coletam informações sobre a forma como os usuários visitam o site ou outros aplicativos, quais páginas eles visitam e quando visitam tais páginas, bem como outros sites que foram visitados antes, dentre outras.

2.3. PRESSUPOSTOS DE APLICAÇÃO

Os dados coletados pelo Cartório, sejam cadastrados nesta Plataforma ou sejam os que venham a compor sua base de dados físicos ou eletrônicos através do atendimento presencial, referem-se ao exercício de suas atribuições relativas a protesto de títulos e documentos, registro civil de pessoas jurídicas e registro de títulos e documentos. Portanto, são utilizados para viabilizar a realização dos atos de ofício solicitados pelos usuários, através do cumprimento das disposições legais e normativas a eles relativas e, nessa qualidade, independem de autorização específica da pessoa natural que deles for titular.

O usuário que decidir fornecer seus dados pessoais, necessários à prática de qualquer serviço realizado pelo Cartório, declara estar ciente e concordar com os termos descritos neste Manual. A concordância com esta Política de Privacidade é indispensável à utilização do *site* e dos serviços oferecidos pelo 2º Tabelionato de Protesto de Títulos, Registro Civil de Pessoas Jurídicas e Registro de Títulos e Documentos de Goiânia.

2.4. BASES LEGAIS PARA O TRATAMENTO

O tratamento dos dados pessoais pelo Cartório é realizado sob bases legais específicas e adequadas para cada uma das atribuições mencionadas no tópico anterior. Veja abaixo as principais normas aplicáveis:

- Lei nº 8.935/94
- Lei nº 9.492/97
- Lei nº 6.015/73
- Código de Normas e Procedimentos do Foro Extrajudicial da Corregedoria-Geral da Justiça de Goiás
- Provimento nº 61/2017 do CNJ
- Provimento nº 74/2018 do CNJ
- Provimento nº 87/2019 do CNJ
- Provimento nº 88/2019 do CNJ

Com referência aos requisitos autorizativos previstos na LGPD, a fundamentação para o tratamento pode ser assim relacionada:

a) com base no consentimento do usuário (art. 7, inciso I da LGPD);

b) para o cumprimento de obrigação legal ou regulatória (conforme acima relacionado), em especial as resoluções do BACEN referentes aos dados de transações bancárias (art. 7, inciso II da LGPD);

c) 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 (art. 7, inciso V da LGPD);

d) 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 (art. 7, inciso IX da LGPD); e

e) para proteção do crédito (art. 7, inciso X da LGPD), de acordo com a Lei nª 9.492/97 e com o Provimento nº 87/2019 do CNJ.

2.5. FINALIDADES DO TRATAMENTO

O tratamento de dados pessoais tem por finalidade a prestação dos serviços notariais e registrais ou, ainda, o exercício de direito, nos termos da legislação vigente.

A coleta de dados visa, ainda, atuar de forma eficaz e proporcionar melhorias na experiência dos usuários com os serviços oferecidos no site.

A maior parte desses dados é solicitada de maneira explícita por meio de formulários físicos ou eletrônicos. Esses dados serão usados exclusivamente para atender as solicitações enviadas aos serviços prestados por essas ferramentas, de modo a agilizar e cumprir sua finalidade.

As análises estatísticas serão efetuadas para interpretar os padrões de utilização do site e serviços disponíveis, a fim de melhorar, de forma contínua, a prestação dos serviços. A informação estatística resultante não será objeto de qualquer identificação pessoal dos usuários.

Caso ocorram mudanças da finalidade para o tratamento de dados pessoais, não compatíveis com o consentimento original, o titular será informado previamente, garantido o direito de revogar o consentimento, se discordar das alterações.

Nos termos da legislação vigente, são considerados inerentes ao exercício da atividade notarial e de registro: atos praticados em livros mantidos por força de previsão legal, incluídos os atos de inscrição, transcrição, registro, averbação e anotação; comunicação para serventia distinta, para anotação em livro e ato nela mantidos; atos praticados em livros previstos em norma administrativa; informações e certidões; e atos de comunicação e informação para órgão público e para centrais de serviços eletrônicos compartilhados que decorrerem de previsão legal ou normativa.

Veja, com mais detalhes, as finalidades para as quais os dados pessoais serão tratados pelo Cartório:

- Qualificação das partes nos atos relativos ao registro de títulos e documentos, ao registro de pessoas jurídicas e a protesto de títulos e documentos.

- Inscrição, transcrição, registro, averbação e anotação de títulos e documentos nos atos relativos às atribuições do Cartório.
- Envio de notificações extrajudiciais.
- Envio de intimações de protestos.
- Recebimento e envio de documentos eletrônicos para fins de registro e protesto.
- Solicitação de atos e envio de informações e certidões relativas a suas atribuições.
- Consulta de protocolo para acompanhamento on-line dos serviços no *site* do Cartório.
- Consulta de existência ou não de protesto.
- Consulta sobre a situação atual do título.
- Consulta de edital eletrônico.
- Consulta de autenticidade de selos eletrônicos.
- Consulta de autenticidade de certidões.
- Agendamento para fins de atendimento presencial.
- Verificação de autenticidade de documentos e assinaturas digitais recebidos, como medida de prevenção a fraudes.
- Registro das transações financeiras e bancárias relativas aos serviços solicitados tais como cartão de crédito, boleto bancário e meios de pagamento em geral.
- Emissão de notas fiscais para Prefeitura de Goiânia.
- Emissão e envio de selo digital no *site* do Tribunal de Justiça de Goiás.
- Emissão de declaração de operações imobiliárias (DOI) à Receita Federal.
- Emissão de declaração de operações suspeitas ao SISCOAF, nos termos do Provimento nº 88/2019 do CNJ.
- Envio de dados ao SINTER e à Receita Federal.
- Envio de comunicações e informações a outros cartórios, órgãos públicos e para centrais de serviços eletrônicos compartilhados que decorrerem de previsão legal ou normativa, como por exemplo, informações sobre títulos ao IEPTB.
- Gerenciar e responder às solicitações feitas pelos usuários, de acordo com os direitos dos titulares de dados, previstos no art. 18 e seguintes da LGPD.

Para atender aos interesses legítimos do Cartório, os dados pessoais serão tratados para:

- Registro no sistema de Ouvidoria por e-mail, telefone, Whatsapp ou correspondência destinados ao atendimento direto ao público, para pedido de informações, reclamações, elogios, sugestões, dentre outros.
- Análise de estatísticas da Plataforma via Google Analytics, com fim de acompanhar os acessos ao site sem coletar dados que identifiquem os usuários.
- Comunicação aos destinatários sobre a necessidade de pagamento de custas e emolumentos para o cancelamento do protesto.

Sempre com o prévio e expresso consentimento do respectivo titular, os dados pessoais serão tratados pelo Cartório para:

- Cadastro na Plataforma.
- Identificação e/ou autenticação pessoal, para o acesso aos serviços on-line.

- Eventual recuperação de login e senha de usuário.
- Salvar histórico de pesquisas.
- Comunicações ou mensagens por telefone, aplicativos ou endereço eletrônico relativos ao andamento, pendências ou conclusão dos serviços solicitados ao Cartório através do *site*, por meio eletrônico ou no atendimento presencial.

2.6. TIPOS DE DADOS COLETADOS

O tratamento dos dados pessoais pelo Cartório é realizado sob bases legais específicas, adequadas, pertinentes e limitadas às finalidades mencionadas no tópico anterior.

Durante a utilização deste site ou no atendimento presencial ou por meio eletrônico, o Cartório poderá coletar dados e informações de identificação para realização de cadastro em formulário próprio e para a finalidade a que se destina.

As informações e dados coletados podem ser assim relacionados e exemplificadas:

- **Informações para a prática dos serviços extrajudiciais**: nome completo; CPF ou CNPJ; nacionalidade; estado civil, existência de união estável e filiação; data de nascimento; profissão; endereço completo; endereço eletrônico (e-mail).
- **Informações de contato:** incluem qualquer tipo de dado de contato, como por exemplo, nome, endereço eletrônico, números de telefone, números de aplicativos de mensagens.
- **Informações de *login* e senha:** incluem informações para identificar e autenticar em serviços fornecidos pelo Cartório.
- **Informações técnicas:** incluem informações sobre seus equipamentos computacionais ou dispositivos móveis, como registro do endereço IP utilizado para conectar seu computador ou dispositivo à *internet*, incluindo sua localização geográfica, tipo de sistema operacional e do navegador da *web.*
- **Informações demográficas:** incluem informações sobre dados demográficos, como data de nascimento, idade ou faixa etária, gênero, localização geográfica.
- **Informações sobre navegação no *site* e serviços:** incluem informações sobre as páginas e conteúdos do nosso *site* e outras informações estatísticas sobre suas interações, como tempos de resposta a conteúdo e duração do acesso, disponibilidade do serviço etc.
- **Informações de redes sociais de terceiros:** incluem as informações que são compartilhadas ou tornadas públicas sempre que o usuário interage conosco por meio de uma rede social de terceiros. Exemplos: nome da conta, nome completo, endereço de e-mail, gênero, data de nascimento, cidade atual e foto de perfil.
- **Informações financeiras e de pagamento:** quaisquer dos serviços prestados em nosso *site* para atender a uma solicitação de pagamento, mediante coleta de dados financeiros e de pagamento para o seu processamento em conformidade com as leis, normas e os padrões de segurança aplicáveis para a prestação do serviço.

2.7. COMPARTILHAMENTO DE INFORMAÇÕES E DADOS PESSOAIS

A publicidade faz parte da natureza e dos fins dos serviços notariais e registrais (art. 1º da Lei nº 8.935/94), na qual se inclui o dever de expedir certidões (Lei nº 8.935/94, Lei nº 6.015/73, Lei nº 9.492/97 e demais normas aplicáveis).

A par dessa especificidade, as informações e dados pessoais podem ser compartilhados nas seguintes hipóteses:

- internamente, com o pessoal autorizado dos serviços;
- realização de serviços ou atos determinados em lei ou em normativas próprias, como por exemplo: expedição de certidões; envio de selo eletrônico; informação ao COAF ou à Receita Federal; emissão de boleto bancário conforme o BACEN;
- cumprimento de requisições de autoridades judiciais e administrativas;
- integração com cartórios e centrais de serviços eletrônicos compartilhados dos institutos notariais e de registro, relativos aos serviços (por exemplo, IEPTB);
- na atuação em eventual processo judicial, com escritórios de advocacia;
- na investigação de possíveis crimes, com as autoridades competentes;
- na contratação de serviços (por exemplo, hospedagem de dados).

No que se refere ao compartilhamento, asseguramos que:

(i) não compartilhamos dados de que tenhamos conhecimento em razão do serviço notarial e de registro com entidades privadas, salvo mediante autorização legal ou normativa;
(ii) nenhum dado pessoal será cedido, gratuita ou comercialmente, a empresas de marketing;
(iii) exigimos de nossos prestadores de serviço a observância de regras compatíveis com esta política e com a legislação vigente em relação à proteção de dados pessoais.

2.8. DIREITOS DOS USUÁRIOS

Conheça aqui os seus direitos:

- Requisitar a informação sobre se os seus dados são tratados pelo Cartório, e como isso é feito.
- Solicitar o acesso e a confirmação sobre informações pessoais que mantivermos. Para isso, podemos precisar de confirmar sua identidade, após o que forneceremos relatório sobre as informações que estão em nosso poder.
- Revogar, modificar ou negar o seu consentimento a qualquer momento, com exceção dos dados tratados mediante obrigação legal, regulatória ou legítimo interesse, sendo que, após sua notificação, não trataremos mais suas informações pessoais para os fins aos quais elas se destinavam.
- Solicitar a informação sobre eventual possibilidade de não dar o seu consentimento e sobre os efeitos e eventuais consequências negativas em cada caso.
- Requisitar a correção de informações, incompletas ou imprecisas a seu respeito, que estejam em nossa base de dados.
- Requisitar a anonimização, bloqueio ou a eliminação de dados que considere desnecessários para a finalidade que estão sendo utilizados, ou que considere excessivos ou tratados em desconformidade com a LGPD.
- Requisitar que suas informações sejam excluídas de nossos arquivos e sistemas quando não houver nenhuma razão para as manter.

- Requisitar informações a respeito do eventual compartilhamento de seus dados com instituições públicas ou privadas.
- Solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
- Requisitar a exclusão de nossas listas de comunicação para deixar de receber nossas mensagens e e-mail.

Observações importantes:

(i) No atendimento das solicitações acima relacionadas, eventualmente poderemos pedir algumas informações complementares para fins de comprovação da sua identidade, visando garantir a segurança, a privacidade e impedir fraudes. Também poderão ser solicitadas, inclusive por escrito, a identificação da finalidade da solicitação.

(ii) Solicitações de informações em bloco, agrupadas ou segundo critérios não usuais de pesquisa, envolvendo tanto titulares de dados pessoais distintos quanto idênticos poderão ser negadas mediante nota devolutiva fundamentada, quando as circunstâncias da solicitação indicarem tratamento de dados pessoais em desconformidade com a Lei nº 13.709/2018.

(iii) Nos termos das normativas vigentes, as informações não abrangem o conteúdo do ato notarial e de registro e deverão ser prestadas com a advertência de que não produzem efeitos de certidão, não sendo dotadas de fé pública para prevalência de direito perante terceiros.

(iv)Quando aplicável, e mesmo que você optar por excluir seus dados de nossa base de dados, o Cartório poderá reter algum ou todos os seus dados pessoais por períodos adicionais ou por outros prazos definidos e fundamentados em bases legais que justifiquem a retenção de dados, visando o cumprimento de obrigações legais ou regulatórias, para o exercício regular de direitos ou fins de auditoria de diversas naturezas.

(v) O Controlador não se equipara ao fornecedor de serviço ou produto para efeito de portabilidade dos dados pessoais a outro fornecedor.

(vi)O encarregado entrará em contato em até 48 horas úteis, e ainda que algumas solicitações possam não ser respondidas de forma imediata, as mesmas serão respondidas em prazo razoável e em conformidade com a legislação aplicável.

2.9. SEGURANÇA DOS DADOS

Em conformidade com os princípios da LGPD e com as boas práticas de segurança da informação e de proteção de dados pessoais, o Cartório assegura que os dados pessoais coletados são tratados de forma íntegra e segura, de acordo com padrões e normas técnicas e administrativas de segurança da informação, confidencialidade e integridade, pelo tempo necessário para realizar as finalidades para as quais foram coletados ou para cumprir os requisitos legais aplicáveis.

O Cartório **possui controle interno acerca do acesso às suas informações através de controles de acesso por biometria, todos os procedimentos executados por nossos colaboradores são documentados e fazemos treinamentos técnicos e comportamentais com nossa equipe acerca do uso adequado e seguro das ferramentas disponíveis.**

Os dados pessoais tratados pelo Cartório são considerados sigilosos e somente serão acessados por pessoas autorizadas e capacitadas para lhes conferir o tratamento adequado, conforme medidas de segurança adequadas para a proteção contra acesso não autorizado, alteração, divulgação ou destruição de dados pessoais coletados e armazenados.

Conforme previsto na legislação, as medidas de segurança existentes consideram a natureza dos dados e de tratamento, os riscos envolvidos, a tecnologia existente e sua disponibilidade. No entanto, em que pesem nos esforços, é preciso ter presente que nenhum sistema é completamente seguro.

É importante observar que este site poderá oferecer acesso a *links* e *frames* de outros sites cujos conteúdos e políticas de privacidade não são de responsabilidade do Cartório, pelo que recomendamos sempre a consulta das respectivas políticas de privacidade ao serem redirecionados para sites externos ou serviços de terceiros disponibilizados por intermédio desta plataforma.

O acesso aos serviços deste site pelo usuário cadastrado é exclusivo pelo ambiente de login, sendo esse e a senha de uso individual e de responsabilidade do usuário. Por isso, reforçamos os cuidados no sentido de não os repassar ou compartilhar com terceiros, nos ajudando, assim, a manter um ambiente seguro para todos.

Caso identifique, tome conhecimento ou suspeite de algo que comprometa ou possa comprometer a segurança dos seus dados, entre em contato com o encarregado nos canais descritos no item 12.

2.10. COOKIES E TECNOLOGIAS DE MONITORAMENTO

Algumas tecnologias de monitoramento, como *cookies, pixels, web beacon* e ferramentas de *analytics* poderão estar presentes no site e em dispositivos.

As informações coletadas por meio de tais tecnologias são utilizadas para realizar métricas de performance do aplicativo, identificar problemas no uso, captar o comportamento dos usuários de forma geral e coletar dados de impressão de conteúdos.

2.11. INCIDENTE DE SEGURANÇA DOS DADOS

Em caso de incidente de segurança que envolva dados pessoais, as medidas técnicas e de segurança serão tomadas em conformidade com a natureza e a extensão dos riscos envolvidos e as comunicações contendo a descrição dos riscos, titulares envolvidos e medidas técnicas e de segurança adotadas para o tratamento do incidente serão realizadas conforme a legislação e as normas aplicáveis.

2.12. CONTATO COM O ENCARREGADO

Se você acredita que seus dados pessoais foram usados de maneira incompatível com esta Política de Privacidade ou com as suas escolhas enquanto titular desses dados ou, ainda, se você tiver dúvidas, comentários ou sugestões relacionadas a esta Política, entre em contato conosco através do encarregado (Data Protection Officer - DPO), que está à disposição nos seguintes endereços de contato:

- DPO: Vivianne Felipe de Brito
- Endereço: Rua 6, nº 225, Centro. Goiânia/Go. CEP: 74023-030
- E-mail (endereço eletrônico): encarregado@2prtd.com.br
- Formulário eletrônico (clique *aqui)*

2.13. ATUALIZAÇÕES E DISPOSIÇÕES FINAIS

O presente Manual de Política de Privacidade e de Proteção de Dados poderá sofrer alterações, especialmente quando houver publicação de novas recomendações pela ANPD ou determinações legais ou administrativas pelos órgãos competentes, vez que os mesmos poderão emitir novas diretrizes ou orientações sobre os temas e procedimentos descritos neste documento.

O Cartório também poderá atualizar esta Política sempre que incorporar novos funcionalidades e serviços, visando proporcionar melhorias na experiência dos usuários.

As atualizações serão feitas mediante a publicação da nova versão e a identificação da data da última atualização, a partir da qual serão imediatamente válidas e aplicáveis.

As mudanças significativas serão comunicadas pelos canais disponíveis e convidamos você a revisitar este documento com alguma periodicidade para estar sempre atualizado sobre as mudanças pontuais.

3. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

3.1. OBJETIVO

Definir o Plano de Resposta a Incidentes de Segurança com Dados Pessoais (doravante também denominado "PRI") do 2º TABELIONATO DE PROTESTO DE TÍTULOS, REGISTRO CIVIL DE PESSOAS JURÍDICAS E REGISTRO DE TÍTULOS E DOCUMENTOS DE GOIÂNIA (o "Cartório").

Cumprir o Código de Normas e Procedimentos do Foro Extrajudicial da Corregedoria Geral do Estado de Goiás, com enfoque especial ao art. 1.340 daquele diploma.

Atender aos princípios da segurança e da prevenção da Lei nº 13.709/2018 (LGPD) como instrumento integrado às regras de boas práticas e de governança do Cartório, nos termos do art. 50 da LGPD.

Estabelecer regras específicas que dialoguem com as demais práticas, protocolos e regras de governança estabelecidas em observância aos princípios da efetividade e adequação (Lei nº 8.935/1994), e da segurança, integridade e disponibilidade (Provimento nº 74/2018 do Conselho Nacional de Justiça).

3.2. INTEGRAÇÃO

Este PRI compõe o Controle de Fluxo nos termos do art.1.337,II,"h" do Código de Normas de Procedimentos do Foro Extrajudicial da Corregedoria Geral do Estado de Goiás.

Em seu conhecimento e aplicação devem ainda ser observados a Política de Segurança da Informação (PSI) - que também integra o Controle de Fluxo -, a Política de Privacidade e os demais documentos pertinentes à política de governança do Cartório.

3.3. O QUE É UM INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS

Incidente de segurança de dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento, comunicação ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita que possa ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

É importante notar que, de modo geral, um incidente de segurança abrange qualquer situação em que ocorra a violação de algum dos pilares da Segurança da Informação: a confidencialidade, a integridade e a disponibilidade.

Dentro desse gênero de incidentes estão o que interessam à LGPD, quais sejam, os incidentes que envolvam especificamente dados pessoais.

Dessa forma, pode-se afirmar que nem todo incidente de segurança envolverá dados pessoais, mas todo incidente de dados pessoais será um incidente de segurança.

3.4. O QUE FAZER DIANTE DE UM INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS

Conforme estipulado na Política de Segurança da Informação (PSI), o Cartório disporá de uma estrutura formalmente constituída de governança em que se destacam as seguintes funções: Operadores, Encarregado, Equipe de Resposta a Incidentes, Comitê de Segurança da Informação e Controlador.

Em caso de incidentes de segurança, os referidos atores deverão observar os procedimentos descritos nos itens seguintes, conforme seus papéis e responsabilidades.

3.4.1. **RECEBIMENTO DA NOTÍCIA E TRIAGEM INICIAL:** a notícia inicial de um possível incidente pode vir de várias fontes, tais como colaborador, parceiros, autoridades legais, administrativas ou institucionais (como Centrais de Serviços Eletrônicos Compartilhados, por exemplo, o IEPTB), mídia, redes sociais, ferramentas e monitoramento, etc. Do mesmo modo, a notícia pode vir de vários canais, tais como: canal de comunicação junto ao titular dos dados (encarregado@2prtd.com.br), canal de comunicação interno (csi@2prtd.com.br), tanto formal quanto anonimamente. Uma vez recebida a notícia, caso o Encarregado não a tenha recebido pessoalmente, ela deverá ser reportada imediatamente ao Encarregado. Esse, por sua vez, deverá acionar a Equipe de Resposta para a triagem inicial, sem prejuízo das comunicações dos Operadores diretamente ao Controlador. Em razão do imperativo da celeridade no tempo da resposta, a triagem inicial deverá se ater à seguinte questão: Ocorreu um incidente de segurança relacionado a dados pessoais?

3.4.2. **AVALIAÇÃO DO INCIDENTE:** realizada a triagem inicial e confirmado o evento adverso, deverá ser acionado o Comitê de Segurança da Informação (CSI) e informado o Controlador, com o objetivo de avaliar mais detalhadamente o incidente, inclusive sobre a necessidade de comunicação com base na seguinte questão: Há risco ou dano relevante aos titulares dos dados?

Ressalte-se, aqui, que em razão do disposto no art. 1.340 do Código de Normas e Procedimentos do Foro Extrajudicial da Corregedoria Geral do Estado de Goiás, o CSI deverá produzir, conforme o caso e em tempo hábil, documento denominado Relatório de Incidente de Segurança com Dados Pessoais que deverá conter minimamente as seguintes informações: *esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.* Elaborado

o referido Relatório e com sua entrega ao Controlador, o Comitê de Segurança da Informação deverá se aprofundar nos seguintes aspectos, a seguir relacionados a título exemplificativo, e não restritivos:

- Qual foi a causa do incidente de segurança?
- Quais foram as vulnerabilidades exploradas que levaram ao incidente?
- Houve uso de credenciais ou acessos comprometidos? Quais são essas credenciais e acessos?
- Quais sistemas, equipamentos e redes foram comprometidos?
- Quais departamentos e atividades foram afetados?
- Quais dados foram afetados?

3.4.3. **COMUNICAÇÃO:** a comunicação do Controlador ao Corregedor Permanente deverá ser realizada no prazo máximo de 24 (vinte e quatro) horas, com o esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados, conforme disposto no art. 1340 do Código de Normas e Procedimentos mencionado em itens anteriores.

3.4.4. **CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO:** As medidas relativas a esse tópico estão intimamente relacionadas às normas do Provimento nº 74/2018 e ao Plano de Continuidade estabelecido pelo Cartório em cumprimento a essa normativa, podendo seu escopo ser assim descrito:

Após a identificação e análise de um incidente, o mesmo deve ser contido e isolado para que outros sistemas não sejam afetados e para evitar maiores danos. Isso implica atuar na raiz do problema e estabelecer as formas de contenção conforme o incidente específico (contenção de curto prazo, backups do sistema e contenção a longo prazo) e preservando-se os registros (trilhas) das evidências do que ocorreu, conforme exigido no mencionado Provimento. Após a contenção da ameaça, a próxima etapa se concentrará na erradicação, ou seja, na remoção da ameaça e restauração dos sistemas afetados. Em sequência, o enfoque será na recuperação dos sistemas afetados, que retornarão ao ambiente de produção após testes e validações para garantir que nenhuma ameaça permaneça.

3.4.5. **MITIGAÇÃO DE NOVOS RISCOS E IMPACTOS:** Essa etapa será dedicada a uma análise crítica da situação para identificação de eventuais vulnerabilidades, dificuldades e melhorias necessárias tanto para o cumprimento do art. 1340 do Código de Normas quanto para subsidiar a tomada de decisão visando o aprimoramento de processo, sem prejuízo das eventuais reparações de danos cabíveis.

3.5. GESTÃO DO PLANO DE RESPOSTA

O Plano de Resposta a Incidentes de Segurança com Dados Pessoais é aprovado pelo Comitê de

Segurança da Informação, em conjunto com o Titular do Cartório.

Membros do Comitê de Segurança da Informação:

- Christiane Costa e Silva de Castro Helou
- Hugo Alexandre Costa e Silva de Castro
- Valber Borges Marinho
- Vivianne Felipe de Brito
- Regis Wellington Miranda Oliveira
- Douglas Godoi Santos
- Agnaldo Rosa de Souza
- Pedro Henrique Carvalho Silva