**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONTROLE DE FLUXO DE DADOS**

**1. Introdução**

O **6º TABELIONATO DE NOTAS DE CAMPO GRANDE/MS** tem como missão servir com eficiência e agilidade, oferecendo uma prestação de serviços de excelência ao usuário.

O Cartório entende que a informação é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados a seus clientes.

O Cartório compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas e privacidade de dados pessoais, seja de clientes ou funcionários.

Dessa forma, esta serventia extrajudicial estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo estabelecer as práticas de segurança da informação para garantir a confidencialidade, integridade e disponibilidade dos dados armazenados pelo Cartório Guarabira.

**2. Objetivo**

Declarar formalmente, as diretrizes do **6º TABELIONATO DE NOTAS DE CAMPO GRANDE/MS**, que visam à proteção dos ativos de informação e privacidade dos dados pessoais com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e 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 o negócio.

Estabelecer as competências, responsabilidades e limites de atuação dos colaboradores do **6º TABELIONATO DE NOTAS DE CAMPO GRANDE/MS**R, em relação à segurança da informação e privacidade, reforçando a cultura de segurança e priorizando as ações necessárias conforme o negócio.

**3. Abrangência de Aplicação**

Esta Política de Segurança da Informação é um documento interno, com valor jurídico e aplicabilidade imediata, plena e indistinta. Ela é aplicada a todos os empregados, estagiários, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores, clientes, menores aprendizes, ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as informações e os ativos deste Tabelionato.

**4. Princípios**

Nosso compromisso com a segurança da informação deste Tabelionato e de nossos usuários está fundamentado nos seguintes princípios e aspectos:

* **Confidencialidade**: toda informação deve ser protegida em todo o seu ciclo de vida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas autorizadas; resguardados os casos de publicidade e compartilhamentos previstos em lei, incluindo meios para garantir a privacidade e a proteção de informações proprietárias.
* **Integridade**: toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
* **Disponibilidade**: toda informação deve estar disponível aos seus titulares de forma oportuna e confiável.
* **Autenticidade**: toda informação trocada tem garantia da identidade de usuário ou sistema de informações com o qual se vai estabelecer comunicação (ser autêntico, ser quem diz ser).
* **Conformidade**: toda informação deve cumprir obrigações institucionais com stakeholders e com aspectos legais e regulatórios relacionados à administração deste Tabelionato, dentro de princípios éticos e de conduta estabelecidos com a alta direção.
* **Assegurar que a Tecnologia da Informação realize a gestão e a segurança dos ativos deste Tabelionato** ou dos que estão sob sua responsabilidade.
* Estabelecer um **plano anual de capacitação e conscientização** direcionado ao desenvolvimento e manutenção das habilidades e aperfeiçoamento dos colaboradores sobre tecnologia e segurança da informação.
* **Cumprir a legislação vigente** no Brasil e demais instrumentos regulamentares relacionados às atividades profissionais no que diz respeito à segurança da informação e aos objetivos institucionais, morais e éticos deste Tabelionato**.**

**5. Diretrizes**

* **Interpretação:**  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 do negócio à época de sua solicitação.
* **Publicidade:** divulgados aos seus colaboradores, visando a sua disponibilidade para todos que se relacionam com este Tabelionato, 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 deste Tabelionato, independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade legal para a qual foi autorizada.
* **Propriedade Intelectual:** é vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual e futuro, deste Tabelionato 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 por este Tabelionato 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. É de responsabilidade do proprietário do ativo classificar as informações como:
* Pública: informações públicas, que podem ser divulgadas publicamente, com acesso irrestrito.
* Interna: informações internas, que podem ser divulgadas a todos os colaboradores e a prestadores de serviços (quando necessário e desde que estes estejam comprometidos com a confidencialidade da informação).
* Restrita: informações restritas, que devem ser divulgadas somente a determinados grupos, áreas ou cargos.
* Confidencial: informações confidenciais, que sua divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação e imagem deste Tabelionato. A informação deve ser divulgada somente a determinados indivíduos.
* **Sigilo:** é vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade deste Tabelionato 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 deste Tabelionato 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 pela TI e por este Tabelionato, sejam eles onerosos, gratuitos, livres ou licenciados.
	+ Todos os ativos em uso no ambiente corporativo devem atender às recomendações de seus fabricantes ou desenvolvedores, especialmente o Provimento 74-CNJ, no que diz respeito à manutenção, atualizações e correções de falhas técnicas de segurança.
* **Acesso à internet:** Este Tabelionatodisponibiliza acesso à Internet para uso nas atividades profissionais de seus usuários, que devem utilizá-lo com responsabilidade, evitando sites suspeitos e que vão contra o bom costume e/ou a legislação vigente. O ambiente de Internet pode ser monitorado para garantir a segurança da informação.
* **Correio Eletrônico:** O correio eletrônico disponibilizado por este Tabelionato deve ser utilizado de forma profissional, ou seja, suas mensagens devem ser escritas com linguagem formal, respeitando os regulamentos internos e a legislação vigente. A conta de correio eletrônico é de responsabilidade do usuário ao qual foi disponibilizada. O conteúdo do correio eletrônico disponibilizado por este Tabelionato pode ser monitorado e acessado pelo quando detectadas situações de risco à segurança da informação, não garantindo ao usuário sigilo das mensagens da conta de correio eletrônico disponibilizadas.

**Obs.:** O acesso e utilização dos ativos disponibilizados por este Tabelionato ou de ativos específicos e/ou particulares, inclusive de forma remota, fora do horário normal do expediente, incluindo, mas não se limitando a, correio eletrônico institucional, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição do Cartório Guarabira.

* **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 deste Tabelionato deve ocorrer somente após solicitação formal e fundamentada do colaborador solicitante e autorização expressa do seu gerente e da 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 deste Tabelionato, salvo 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 deste Tabelionato,tais como, Whatsapp, Facebook Mensenger, Instagram Mensenger, Telegram, dentre outros.
* **Mídias Sociais:** A participação do colaborador nas mídias sociais por meio dos ativos deste Tabelionato 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.

**6. Controle de acesso**

 Este Tabelionato controla o acesso físico, lógico e virtual às suas dependências, aos seus ativos e equipamentos de informática, através das seguintes práticas:

* A identificação de qualquer colaborador ou prestador de serviço deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.
* Sua senha deve ser mantida secreta, sendo proibido o seu compartilhamento.
* As solicitações para concessão e revogação de acessos físicos e lógicos devem ser registradas formalmente.
* Os acessos devem ser revisados periodicamente.
* O acesso deve ser retirado logo após o encerramento/mudança das atividades, contratos ou acordos com colaboradores e prestadores de serviço.
* A concessão de acesso e o uso de acessos privilegiados devem ser restritos e controlados.

**6.1. Gestão de Acesso aos Sistemas e Ambientes**

* **Ambientes Lógicos:** os sistemas e processos que suportam os ativos deste Tabelionato devem ser confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais.Qualquer acesso à informação e às funções dos sistemas deve ser autorizado, registrado e restrito, podendo até mesmo ser rastreado. O acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (login).
* **Ambientes Físicos:** este Tabelionato estabelece perímetros de segurança para proteção de suas propriedades, bem como implementar controles de identificação e registro de acesso em suas dependências para assegurar o acesso somente de colaboradores autorizados e ativos homologados.Os perímetros de segurança devem ser protegidos com controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
* Este Tabelionato deve diminuir os riscos relacionados à mídia em papel, armazenamento removível e recurso de processamento da informação sem monitoramento.
* **Áudio, Vídeos e Fotos:** É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências deste Tabelionato por seus colaboradores, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico ou uso nas mídias sociais.

**7. Remoção de Ativos**

Os recursos deste Tabelionato, sendo eles equipamentos, informações ou software não devem ser removidos sem autorização prévia do gestor responsável pelo colaborador ou prestador de serviço.

Os softwares de segurança, como antivírus e patches de segurança, não devem ser desinstalados sem a autorização prévia do gestor de segurança da informação.

**7.1. Descarte**

O descarte dos ativos deste Tabelionato deverá ser realizado seguindo as diretrizes da Corregedoria Geral de Justiça do Estado da Paraíba, CNJ e legislações específicas, especialmente o provimento 50/2015 do Conselho Nacional de Justiça.

**8. Estações de Trabalho**

Os dados sensíveis ou críticos, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro quando não estiverem em uso, especialmente quando as dependências físicas estiverem desocupadas. Quando em uso, o colaborador deverá tomar as medidas de segurança para evitar o vazamento ou uso indevido dos dados.

Os recursos de processamento de informação (computadores, notebooks, servidores, etc) devem ser mantidos desligados ou protegidos com mecanismo de tecla de bloqueio, senhas ou outros controles, quando não usados.

Os documentos que contêm informação sensível ou classificadas como restrita ou confidencial devem removidos das impressoras e digitalizadoras imediatamente após o uso ou impressão.

**9. Trabalho Remoto**

Este Tabelionato permite o trabalho remoto, desde que autorizado pelo gestor imediato e pelo gestor de segurança da informação, seguindo as premissas:

* Em casos de acesso remoto para suporte técnico ao ambiente de processamento de dados, o acesso deve ser realizado através de VPN criptografada.
* Para o acesso aos demais serviços em nuvem, a estação cliente deve ter o mínimo de controles instalados, como antivírus e conexão confiável.
* O período de trabalho remoto deve estar em conformidade com o contrato de trabalho ou prestação de serviço.

**10. Contratação, Terceirização ou Prestação de Serviços:**

Os relacionamentos e contratações, inclusive de colaboradores, em que ocorra o compartilhamento de informações deste Tabelionato 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.

**10.1. Auditoria junto aos prestadores de serviço**

Cláusulas contratuais que dispõem sobre a realização de auditorias eventuais ou periódicas para certificar a conformidade com a PSI e seus documentos complementares devem ser estabelecidas junto aos prestadores de serviço deste Tabelionato.

**10.2. 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.

**11. Cópias de Segurança**

* **Documentação**: este Tabelionato deve possuir documentação adequada e suficiente para garantir a compreensão e rápida recuperação em situações de contingência de seus sistemas e processos que envolvam seus Ativos.
* **Salvaguarda (backup):** este Tabelionato 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.

**12. Gestão de Vulnerabilidades Técnicas**

* **Análise dos processos e Ativos:** este Tabelionato 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**: este Tabelionato 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, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.
* **Inspeção dos Ativos**: este Tabelionato, 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, independentemente da interação com seus ambientes e informações.

**13. Gestão de Configuração e Mudança**

O andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica deste Tabelionato devem preservar os controles relacionados à disponibilidade, integridade, sigilo e autenticidade das informações.

**14. Conformidade**

Este Tabelionato 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.

**15. Continuidade do Negócio**

No escopo das ações de segurança da informação e privacidade, 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.

**16. Capacitação**

Este Tabelionato deve possuir pessoas capacitadas para exercer a conscientização em

segurança da informação e privacidade para capacitação e disseminação da cultura de segurança da informação, proteção de dados e privacidade junto aos seus colaboradores.

**17.** **Investimentos**

Os investimentos em segurança da informação e privacidade deste Tabelionato 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.

**18. Segurança nas comunicações**

Qualquer comunicação que trafegue informações para o negócio deve adotar mecanismos para que a Segurança da Informação seja garantida.

O compartilhamento de ativos deverá ser feito estritamente dentro dos autorizativos legais. Toda informação, processada internamente ou transmitida para organizações externas, deve estar protegida por meio de uma operação segura e pela correta utilização dos ativos de informação.

As informações trafegadas em mensagens eletrônicas devem ser adequadamente protegidas.

**19. Gestão de Incidentes**

Este Tabelionato possui 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.

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 deste Tabelionato.

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.

Qualquer dúvida relativa a esta PSI, bem como para notificação e registro de incidentes de Segurança da Informação deve ser encaminhada ao CSI por meio do e-mail lgpd@6cartoriocg.com.br

**20. Penalidades**

**20.1. Violações**

Os incidentes de segurança da informação devem ser avaliados pelo CSI, Cartório Guarabira. Ao constatar uma violação, o CSI deverá avaliar o caso, podendo instaurar e apurar as responsabilidades dos envolvidos em procedimento administrativo disciplinar, visando aplicação de sanções administrativas cabíveis previstas em cláusulas contratuais, regimento pessoal e outros documentos normativos do cartório, além da legislação vigente.

Verificada a ocorrência de incidente com dados pessoais, o CSI comunicará ao encarregado para que promova à comunicação ao Juiz Corregedor Permanente da Comarca ou Corregedoria Geral de Justiça no prazo de 24h.

Sem prejuízo, os incidentes de segurança com dados pessoais serão imediatamente comunicados pelo CSI ao controlador.

**20.2. Tentativa de Burla**

A tentativa de burlar às diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

**21. Papéis e Responsabilidades**

**21.1. 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.

**21.2. 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 corretivas para reduzir o risco;
* Tomar as ações cabíveis para se fazer cumprir os termos desta política;
* Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

**21.3. Controlador nomeado**

* Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, 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 informações geradas ou sob a responsabilidade da sua área, ajustando a classificação e rotulagem dessas 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.

**21.4.** **Encarregado nomeado**

* 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).

**21.5. Colaboradores**

* Seguir as diretrizes e aspectos estabelecidos nesta política;
* Conhecer e cumprir as políticas e procedimentos de Segurança da Informação;
* Ser responsável pelo uso adequado e seguro dos ativos de informação e das informações a que tenha acesso;
* Buscar orientação sempre que não estiver absolutamente seguro quanto ao manuseio das informações;
* Comunicar ao Comitê Gestor de Segurança da Informação casos de violação ou falhas relacionadas à Segurança da Informação.
* Manter a confidencialidade de suas senhas, não as compartilhar e criá-las obedecendo os requisitos de complexidade exigidos na Política de Controle de Acesso.
* Devolver o ativo de informação após o encerramento de suas atividades, do contrato ou acordo.

**21.6. Usuários**

* Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
* Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos a TI ou, quando pertinente, ao CSI;
* Comunicar à TI qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações e privacidade do cartório;
* Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições

**21.7. 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 entregar a PSI na ocasião da admissão do novo colaborador e colher assinatura no documento “Termo de Compromisso para colaborador interno”;
* Realizar a guardar o documento na pasta funcional do colaborador;
* Disponibilizar e realizar a gestão das credenciais individuais de acesso ao ambiente físico do cartório.

**22. Gestão da Política**

A Política de Segurança da Informação é aprovada pelo Comitê de Segurança da Informação, em conjunto com a Tabeliã de Notas.

Campo Grande/MS, 02 de maio de 2024.

**ISABELA TAVARES SCHNAIDER**

TABELIÃ DE NOTAS