Colégio Notarial do Brasil
CONSELHO FEDERAL

MANUAL DE BOAS PRÁTICAS DO AMBIENTE TECNOLÓGICO DO NOTARIADO

Sumário

Apresentação

Este manual de boas práticas do ambiente tecnológico do Notariado foi elaborado pelo Colégio Notarial do Brasil, Conselho Federal – CNB, com o objetivo de estabelecer diretrizes básicas e procedimentos de gestão dos ativos tecnológicos dos Tabelionatos de Notas para a adequada segurança da informação dos atos notariais brasileiros.

A utilização de recursos tecnológicos no mundo atual é cada vez inerente e mandatória na operação das organizações, tendo um papel estratégico no desenvolvimento e manutenção de sua competitividade. No caso dos Tabelionatos de Notas, o uso de sistemas e processos adequados têm impacto direto na qualidade da prestação dos serviços aos cidadãos, trazendo agilidade, controle e segurança das informações.

O CNB, em sua missão institucional, entende que a interconexão dos Tabelionatos de Notas é imperativa e colaborará para aperfeiçoar os serviços, ampliando-os e facilitando o acesso da população e dos poderes públicos aos dados coletados pelos serviços notariais.

O objetivo futuro do CNB é:

- Prover todos os cartórios de notas com equipamentos e aplicativos disponíveis em rede;

- Interligar todos os equipamentos em nuvem, onde a proteção de rede e dados possa ser robusta;

- Prover sistemas e aplicativos padronizados, que possam ser utilizados pelos tabeliães, seus funcionários e pela população em geral, presencial ou remotamente;

- Coletar informações biométricas que permitam o serviço de autenticação de biometria.

Com o constante avanço tecnológico na atualidade, os aspectos de segurança da informação tornam-se cada vez mais complexos, exigindo métodos de

[1] https://me-en.kaspersky.com/about/press-releases/2017_employees-hide-it-security-incidents- in-53-of-business-in-the-uae

segurança sofisticados. Há estatísticas que reportam que mais de 46% dos incidentes de segurança são causados pelos próprios funcionários da empresa1. Além disto, ataques cibernéticos são uma ameaça constante às redes de computadores, impactando não só uma organização, mas disseminando em escala global.

A política de segurança é um conjunto de regras a serem seguidas por todos os utilizadores dos recursos tecnológicos do Tabelionato de Notas, abrangendo todos os colaboradores, prestadores de serviço e qualquer outra pessoa em que seja necessário liberar um acesso ao ambiente computacional e/ou aos respectivos sistemas
e aplicativos.

Operação do Tabelionato

A estrutura tecnológica para a operação do tabelionato poderá variar conforme o porte, tipos de sistemas utilizados e tecnologias adotadas. A realidade atual apresenta um ambiente bastante heterogêneo, com Notários bastante informatizados e outros com poucos recursos tecnológicos.

Os principais recursos tecnológicos para a operação do Tabelionatos de Notas são:

Hardware

* **Computadores:** os funcionários dos Notários deverão ter à disposição computadores para a operação do fluxo de trabalho do cartório, devendo ao menos para as funções de registro dos atos notariais. É fundamental que a versão do sistema operacional instalado tenha suporte ativo do fabricante.

* **Impressoras e scanners:** a impressão e digitalização de documentos são ferramentas fundamentais na operação do tabelionato. Equipamentos conjugados denominados multifuncionais são uma boa opção de custo benefício.

• **Servidores:** São o elemento central da rede de computadores, fornecendo serviços às estações de trabalho. A utilização de servidores para a operação do Tabelionato de Notas garante maior segurança, disponibilidade e performance. Conforme o tamanho do Tabelionato, pode-se definir servidores específicos para a aplicação (sistema de gestão), gerenciador de banco de dados, correio eletrônico, antivírus, dentre outros.

• **Roteador:** utilizado para controlar as conexões externas (internet) e internas (rede interna)

• **Switch:** equipamento para a conexão de equipamentos na rede interna do tabelionato através de cabeamento RJ45, permitindo interligar estações de trabalho com servidores, impressoras, dentre outros equipamentos.

• **Nobreak:** o nobreak é um equipamento que através de baterias visa proteger a operação dos equipamentos contra oscilações e quedas de energia. Desta forma, mantém os equipamentos ligados ao dispositivo quando a alimentação normal é interrompida, sem riscos de perda de dados. Recomenda-se adotá-los em equipamentos com missão crítica, principalmente servidores e eventualmente algumas estações de trabalho, respeitando a capacidade máxima informada pelo fabricante do nobreak. Deve-se considerar também que estes equipamentos têm vida útil, assim como as baterias de automóveis, e, portanto, precisam passar por manutenção periódica.

• **Leitor biométrico:** os leitores biométricos permitem a coleta das digitais de uma pessoa. A coleta pode ocorrer no processo de abertura de firmas, que poderão ser validadas a cada realização de um novo ato, efetuando a captura e comparação com a previamente armazenada no banco de dados do sistema.

• **Webcam:** a utilização de webcam servirá para coletar a fotografia das pessoas e, opcionalmente, a identificação facial biométrica. Também será um recurso importante para coleta e comparação da identificação de pessoas nos atos notariais.

• **Tablet para assinatura biométrica:** a assinatura biométrica é um recurso que mede pelo menos seis fatores da assinatura de uma pessoa. A saber: pressão, velocidade, ritmo, aceleração, inclinação e torção. O dispositivo para a assinatura biométrica poderá ser através de um tablet específico para este fim ou alguns modelos voltados ao consumidor comum para uso genérico, encontrado em diversas lojas do país, mas que tenham determinadas especificações que permitam a coleta dos fatores da assinatura biométrica.

Software Base

• **Sistema Operacional:** sistema básico de operação de todos os softwares e aplicativos do ambiente de rede. Os sistemas operacionais mais conhecidos são Windows e Linux, com as respectivas variações de versões para desktop e servidor. No caso de Linux, também há diferentes distribuições construídas a partir de seu núcleo, tais como, Ubuntu, CentOS, Debian.

• **Serviço de diretório:** serviço que identifica todos os recursos disponíveis na rede e faz o gerenciamento unificado de acessos a usuários e aplicações para cada recurso identificado. Dentre algumas soluções de mercado, destacam-se: Microsoft Active Directory, Apache Directory, Open LDAP.

• **Banco de Dados:** os gerenciadores de bancos de dados mais utilizados atualmente são Oracle, SQL Server, MySql e PostgreSQL. Há também outros tipos de bancos orientados a documentos, tais como, MongoDB e Cassandra. Normalmente, a definição do banco de dados a ser utilizado no Tabelionato de Notas será de acordo com o aplicativo de gestão de cartórios em uso.

• **Antivírus:** softwares especialistas que previnem a entrada de vírus no ambiente computacional do Tabelionato de Notas.

• **Anti-Ramsomware:** ferramenta que previne o ataque de Ramsomware que sequestra o equipamento infectado, criptografando seus dados e somente liberando sob pagamento de resgate.

• **Firewall:** dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança de acesso externo a esta rede de computadores.

• **Software para backup:** software que garante a cópia do ambiente e dados do Tabelionato de Notas.

Aplicativos

• **Sistema de Gestão de Cartórios:** os Tabelionatos de Notas, em geral, operam através de sistemas de gestão de cartórios que são, na maioria dos casos, soluções comercializadas por fornecedores de software que atuam no segmento de cartórios. Os sistemas de gestão de cartórios têm como principais funcionalidades:

a) controle de pedidos realizados no balcão
b) sistematização das etapas de elaboração do ato notarial
c) gestão financeira
d) armazenamento dos dados do ato notarial em meio eletrônico
e) repositório de imagens dos documentos
f) possibilidade de backup do banco de dados do sistema

• **Aplicativos de automação de escritórios:** composto mais comumente por processador de texto, planilha eletrônica, software para apresentações e correio eletrônico. As soluções mais conhecidas são Microsoft Office, G Suite, LibreOffice, WPS Office e Apache Open Office.

Serviços

• **Link de Internet:** embora muitos Notários já possuam link de internet contratados, o que permite o envio de informações à CENSEC, Receita Federal e obrigações dos estados, haverá a necessidade de uma conexão com boa disponibilidade com a implantação do ato notarial eletrônico. Para as regiões onde a infraestrutura local é restrita para uma internet de boa qualidade, recomenda-se ao Notários sempre manterem-se atualizados sobre

as alternativas que a região oferece, buscado aumentar a qualidade das conexões. Há soluções denominadas Aceleradores WAN que otimizam o tráfego de informações, compactando os dados e enviam apenas as diferenças e não todo o bloco de conteúdo.

• **Conexão à Internet:** serviço que permite acessar os endereços de internet através dos computadores e dispositivos conectados na rede interna criada pelo Tabelionato de Notas.

• **Rede sem fio:** permite a conexão à rede interna do Tabelionato de Notas e internet através de conexão sem fio (wireless). A gestão das redes internas ocorre normalmente através de um roteador. Pode-se criar mais de uma rede interna sem fio para uso restrito aos funcionários do Tabelionato de Notas e outra para clientes com acesso exclusivo à internet, por exemplo.

• **Backup remoto:** permite a cópia das informações do Tabelionato de Notas para um provedor externo, diferente do local do servidor principal.

• **Site:** páginas acessadas por um domínio registrado na internet para a apresentação geral do Tabelionato de Notas e divulgação de serviços. As páginas podem ser estáticas, com o objetivo de apresentar conteúdos informativos, ou páginas dinâmicas, que permitem a interação do usuário (cadastramento, solicitação, consultas, etc.) e normalmente necessitam de uma linguagem de programação para serem desenvolvidas.

• **Colocation:** serviço que permite hospedar os servidores próprios do cartório em estrutura de datacenter de terceiros. Conforme o número de equipamentos do Tabelionato de Notas, o fornecedor calculará a área necessária dentro de seu datacenter e cobrará um serviço pela hospedagem e suporte. Outros serviços poderão ser oferecidos complementarmente.

• **Contratação de Nuvem:** serviço que permite o provisionamento de recursos computacionais de forma configurável e ágil, com acesso através da internet. Neste caso, o notário terá menores investimentos em aquisição de infraestrutura própria (Capex), pagando ao provedor pelo uso dos recursos

(Opex). Há três principais modelos de serviço em nuvem:

- **IaaS –** Infraestrutura como serviço: o provedor contratado irá disponibilizar para o uso serviços voltados para infraestrutura, tais como, máquinas virtuais (VMs), backup, redes, servidores de banco de dados. Neste modelo, o notário ficará responsável pela configuração do ambiente, tais como, instalação de servidores de aplicação, sistemas operacionais, certificados, firewall, dentre outros.
- **PaaS –** Plataforma como serviço: é um seviço mais abrangente que o IaaS já que, além de contemplar os serviços do IaaS, o provedor também será responsável pela configuração do sistema operacional, servidores de aplicação.
- **SaaS –** Software como serviço: nesta modalidade, o fornecedor do sistema fica responsável por todo o gerenciamento da infraestrutura. O Notário pagará pelo uso do sistema, sendo que os custos de infraestrutura já estarão embutidos neste valor.

Política de Segurança da Informação

A Política de Segurança da Informação deve atender basicamente aos seguintes requisitos:

• **Confidencialidade:** garantir que o acesso às informações seja efetuado somente por pessoas autorizadas;

• **Disponibilidade:** garantia que as informações estejam disponíveis sempre que necessário para acesso aos usuários autorizados;

• **Autenticidade:** garantir a identidade de um usuário ou sistema com que se realiza uma comunicação;

• **Integridade:** garantir que a informação seja mantida em seu estado original e proteger para que não seja alterada na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

• **Não repúdio:** garantir que um autor não consiga negar falsamente um ato ou documento de sua autoria. Isto é condição necessária para a validade jurídica de documentos e transações.

• **Mecanismos de Segurança**

Os mecanismos de segurança abrangem os aspectos físicos e lógicos do ambiente tecnológico dos Tabelionatos de Notas:

• **Controle Físico**

Os principais exemplos de controle físico são:

- Salas exclusivas para o datacenter, local com acesso restrito;
- Acesso ao datacenter local através de senha, identificação biométrica ou chave sob posse de pessoas autorizadas;
- Câmeras de segurança;
- Vigilantes;
- Restrição de acesso de terceiro no interior da serventia.

• **Controle Lógico**

São barreiras que impedem ou limitam o acesso às informações através de sistemas e da rede de computadores, impedindo a exposição da informação para acesso e modificação por pessoas não autorizadas.

Os controles mais comuns são:

- Firewall;
- Senha individual;
- Configuração de bloqueio de tela (recomendável 5-10 minutos) e configurações de comando do sistema operacional;
- Identificação biometria;
- Certificado digital.

• **Mecanismos de Prevenção**

Para uma adequada política de segurança da informação nos tabelionatos de notas, recomenda-se a adoção dos seguintes mecanismos:

- **Backup**

Manter os dados sempre protegidos é uma condição essencial para garantir a continuidade das operações do tabelionato. Partindo do pressuposto que todo equipamento tem uma vida útil e o ambiente da rede pode ser impactado por ameaças virtuais, é fundamental a adoção de políticas de backup dos dados do tabelionato. Todos os backups devem ser automatizados através de sistemas específicos com opção para agendamento em horários determinados. Os responsáveis pela gestão dos sistemas de backup deverão atualizar periodicamente o sistema com as atualizações disponibilizadas pelo fornecedor do software. Estas atualizações trazem correções e novas funcionalidades que melhorarão a operação. Recomenda-se adotar a regra de backup 3-2-1 que representa ter pelo menos três cópias dos dados, armazená-las em duas mídias diferentes e manter uma cópia de backup fora do local. Há diversões soluções e opções no mercado que podem ser adotadas pelo Notário.

Uma prática recomendada é replicar os dados do servidor do sistema de gestão do Tabelionato de Notas a um outro servidor, com espelhamento em tempo real, tanto em nível de base de dados como de sistema operacional. Esta medida visa minimizar o impacto de uma parada do ambiente principal, não ocasionando interrupções nos serviços notariais.

As mídias de backup físicas (fitas LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro e distantes o máximo possível do Datacenter. Estas devem ser devidamente identificadas para facilitar a eventual recuperação dos dados. Além disto, deve-se controlar a vida útil da mídia, conforme recomendações do fabricante, efetuando migrações para outra mídia quando necessário.

Atendendo às recomendações 9 e 11 do CNJ2, é recomendável que uma das cópias do backup seja transmitida para o ambiente remoto (cloud) em servidores instalados no território nacional. O acesso deve ser realizado com conexão segura e criptografada. O backup deve ser realizado diariamente, de preferência em horário fora do expediente do Tabelionato de Notas, período em que não há operação ou processamento de rotinas de sistemas. Deve-se programar execuções diferenciais ou incrementais, sendo que o backup completo deve ser realizado pelo menos uma vez por semana. As duas últimas cópias, tanto incrementais quanto completas, devem sempre estar disponíveis.

Recomenda-se efetuar testes de restauração (restore) de backup aproximadamente a cada 60 dias visando certificar que o processo não apresenta falhas e identificar pontos que precisam de melhoria no processo. Vale ressaltar que por este ser um procedimento de simulação, os arquivos devem ser restaurados em local diferente do atualmente em uso na operação do Tabelionato de Notas, para evitar a sobreposição indevida dos arquivos.
Há diversas opções de software especializados em backup, licenciados ou gratuitos, além de serviços de hospedagem em cloud. Veja abaixo alguns exemplos de soluções no mercado:

- Licenciados: Backup Exec Symantec, Veeam
- Gratuitos: Comodo, EaseUS Todo, Cobian, Iperius
- Cloud: AWS, Azure, Google Cloud, Mandic

• Snapshot

O snapshot é uma funcionalidade existente nos sistemas de armazenamentos de dados que permite criar imagens dos dados de uma forma muito rápida, com consumo de armazenamento reduzido e mínimo impacto no ambiente de produção, em intervalos de uma hora ou até minutos.
Nas operações com missão crítica com é a dos notários, a criação de snapshots sobre o armazenamento de dados é uma prática bastante recomendada. Somente a execução de backup diário não é suficiente para permitir o restauro de dados importantes, e pode provocar uma perda de informação crucial para o Tabelionato de Notas.

• Senhas de acesso

A definição de políticas internas de senha visa a garantir maior segurança no acesso às informações do Tabelionato de Notas. A política de senhas define as regras que devem ser cumpridas, como comprimento e tipo de caracteres permitidos e não permitidos, além de periodicidade de troca.
Como recomendações gerais, sugere-se as seguintes regras:

- Obrigar o tamanho mínimo e a inserção de letras e números;

Exemplo: a senha deve ter 8 caracteres contendo números, letras maiúsculas e minúsculas;

[2] http://www.cnj.jus.br/recomendacoes-corregedoria

• Adotar um prazo de validade das senhas, obrigando a troca pelo usuário após a expiração. Sugere-se obrigar a troca de senha no máximo a cada 120 dias, sendo usual o máximo de 30 dias;

• Proibir a repetição de caracteres. Por exemplo, se a senha era 'T32xpTo', a próxima senha tem que ter caracteres diferentes;

•Se possível, criar uma lista de senhas que não podem ser utilizadas.

É recomendável ao Notário conscientizar os usuários da rede do Tabelionato de Notas a não usarem na elaboração de uma senha dados pessoais que são obtidos com certa facilidade em cadastros e possivelmente serão alvos de tentativa para descoberta da senha do usuário. Exemplos: nome, sobrenome, números de documentos, telefones, placas de carro e datas.

Por questões de segurança, sempre que disponível, deve-se preferir o acesso a sistemas através de certificados digitais ou biometria ao invés de senha. Entretanto, para uma segurança extra, é recomendável o uso de autenticação por dois fatores, podendo combinar senha com biometria ou mesmo dois tipos diferentes de biometria para identificar a pessoa. Outra possibilidade é tornar o computador ou dispositivo móvel confiável para acesso ao sistema. Neste caso, sempre que ocorrer um acesso ao sistema através de um computador ou dispositivo móvel ainda não cadastrado na lista de confiáveis, será solicitada a digitação de um código de verificação a ser enviado pelo sistema ou obtido por token (exemplo: RSA SecureID).

• Antivirus e Anti-spyware

Na internet há uma série de ameaças desenvolvidas por cyber criminosos que podem afetar a proteção dos dados do Tabelionato de Notas. Neste sentido, a utilização de ferramentas de antivírus deve ser adotada com o objetivo de identificar vulnerabilidades e bloquear ameaças. Antes de adquirir uma ferramenta de mercado, recomenda-se consultar o desempenho através de testes realizados por empresas independentes, tais como, Av-Test e Av-Comparatives 3.

Preferencialmente, o software antivírus deve ser adquirido e instalado na versão servidor com o número de estações conforme a necessidade do Notário. O módulo servidor ficará responsável pelo gerenciamento das estações de trabalho e efetuará a replicação automática das atualizações software.

• **Firewall**

Os firewalls são ferramentas indicadas para proteger a rede do tabelionato contra ameaças virtuais e ataques de hackers, que pode ser através de software e hardware. É uma ferramenta que visa controlar o fluxo da rede, determinando quais informações podem ser transmitidas ou recebidas. Há várias possibilidades de solução de firewall, que dependerá da configuração de cada tabelionato.

Recomenda-se a adoção de firewalls de última geração NGFW (Next Generation Firewalls) aprimorados com pacotes UTM (Unified Threat Management) ativados, pois demandam menos esforço de gerenciamento sem a necessidade de aquisição de produtos complementares. Estas soluções abrangem a capacidade de firewall corporativo, sistema de prevenção de intrusão (IPS) e controle de aplicação.

Os firewalls de última geração vão além dos firewalls tradicionais que tratam de filtragem de pacotes e protocolos, pois são destinados a impedir o crescente número de ataques de aplicativos.

Os Tabelionatos de Notas devem contratar um dos tipos de Firewall e manter a configuração sempre atualizada.

• **Utilizar softwares e aplicativos originais**

A utilização de software não originais deixa os sistemas vulneráveis e o Tabelionato de Notas em risco, pois podem conter componentes maliciosos ocultos (malwares, spywares, etc.), os quais podem roubar informações de documentos, senhas ou outras informações sigilosas.

Com a adoção de software e aplicativos originais, ganha-se o benefício do suporte às atualizações periódicas de segurança, além de melhorias gerais de funcionalidades, disponibilizadas pelos fornecedores de software.

Vale ressaltar, entretanto, a necessidade de migrar para uma nova versão do software original quando o fabricante do software deixar de suportar a versão instalada no Tabelionato de Notas.

Recomenda-se adotar softwares open source que têm a vantagem de custos reduzidos, ou até gratuitos. Deve-se considerar, entretanto, que o custo de suporte para manter o software open source pode ser maior que os softwares de mercado. Além disto, é importante analisar eventuais problemas de incompatibilidade com o software predominante no mercado corporativo, que podem dificultar a operação dos atos notariais.

• **Atualização frequente do sistema operacional e aplicativos**

A atualização periódica dos pacotes de correção e atualização fornecidas pelos fabricantes de software é imprescindível para garantir a segurança da informação do Tabelionato de Notas.

Conforme comentado anteriormente, de nada vale um software original que não tenha um suporte ativo do fabricante, principalmente quanto às questões de segurança contras objetos maliciosos.

• **Navegação consciente da Web e e-mails**

A conscientização de todos os envolvidos no uso de recursos tecnológicos do Tabelionato de Notas é fundamental para garantir a estabilidade e segurança do ambiente computacional. Políticas de acesso e uso de internet e correio eletrônico pelos colaboradores do tabelionato também devem ser explorados visando mitigar riscos de vazamento de informações e invasão de programas maliciosos e vírus na rede interna.

As principais recomendações para a navegação consciente são:

• Não clicar em links recebidos por e-mail (se a comunicação for urgente ou na dúvida, contate o remetente para checar a procedência do envio)
• Não executar arquivos anexados a e-mails, sem antes examiná-los
• Evitar sites que pareçam suspeitos e não clicar em links de janelas Pop-ups
• Utilizar sites seguros ao enviar dados confidenciais

• **Disponibilização da rede sem fio para clientes**

Visando melhorar a percepção de atendimento e propiciar uma comodidade adicional aos clientes, é uma tendência oferecer o acesso à internet, através de rede sem fio, para os clientes do Tabelionato de Notas. Neste caso, recomenda-se criar uma rede sem fio, através do roteador, específica para este fim. Como a respectiva senha de acesso ficará pública, o acesso deve ser restrito à internet, sem, portanto, qualquer possibilidade de acesso aos sistemas administrativos do Tabelionato de Notas. É também importante que a senha seja alterada rotineiramente, de preferência a cada 30 dias.

O roteador utilizado pelo Tabelionato de Notas deve permitir a criação de diversas redes, caso contrário, será necessário adquirir um roteador adicional para a segregação necessária dos acessos.

Adicionalmente, de acordo com a Lei no 12.965/14, art. 13, o administrador da rede deve manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano. Sugere-se armazenar os cadastros realizados, os IPs de conexão, MAC Address dos equipamentos, horários e duração das conexões.

• Pulverização do conhecimento

O Notário deve atentar-se ao nível de dependência do conhecimento de poucas pessoas para a manutenção do ambiente tecnológico do Tabelionato de Notas. É comum os pequenos Tabelionatos dependerem de apenas uma pessoa para cuidar do ambiente, sendo este detentor de senhas de acesso de administrador e único conhecedor dos procedimentos técnicos, os quais muitas vezes não estão documentados. Em caso de ausência deste profissional, o Notário correrá riscos de interrupções nos serviços notariais por desconhecimento destes procedimentos. Além disto, o reestabelecimento dos serviços poderá ser muito moroso.

O Colégio Notarial do Brasil recomenda que sejam adotadas as seguintes medidas visando mitigar os riscos aqui comentados:

• Requisitar ao responsável técnico do Tabelionato de Notas a elaboração de documentação de procedimentos e orientações técnicas do ambiente tecnológico. O objetivo principal desta documentação é tornar o processo impessoal, permitindo que qualquer pessoa com um mínimo de especialização possa entender rapidamente o cenário tecnológico e providenciar os principais procedimentos tanto rotineiros quanto por motivos de falha. É fundamental que esta documentação seja revisada sempre que algum procedimento for alterado.

• Em caso de equipe própria, buscar a formação de pelo menos uma segunda pessoa que manterá o conhecimento da operação técnica.

• No caso de opção por empresa terceirizada, preferir aquelas com equipes mais especializadas e estruturadas. Entretanto, o Notário deverá certificar-se que o conhecimento da operação do ambiente tecnológico do Tabelionato de Notas está sendo difundido por pelo menos mais uma pessoa desta empresa.

• **Recomendações gerais**

Recomenda-se estabelecer alguns procedimentos adicionais na rede do Tabelionato de notas que visam a aumentar o nível de segurança, melhorar a durabilidade dos equipamentos e racionalizar custos.

• Estabelecer termos a serem assinados por todos os colaboradores e usuários do ambiente tecnológico do Tabelionato de Notas, a saber:

• Termo de Responsabilidade e Sigilo (vide anexo 1)

• Termo de Uso para Acesso Remoto (vide anexo 2)

• Termo de Uso sobre Computador Portátil (vide anexo 3)

• Não permitir o compartilhamento de senhas de acesso

• Desligar os computadores, monitores e impressoras ao final do expediente

• Encerrar a sessão ou bloquear a estação sempre que se ausentar da estação de trabalho

• Evitar o desligamento forçado do computador

• Evitar impressão desnecessária e fazer o descarte documentos confidenciais em fragmentadoras

• **Datacenter**

Datacenter é o local onde os servidores do tabelionato ficam concentrados. É uma tendência hospedar os sistemas da empresa em provedores externos, embora a realidade em sua maioria dos notários é ter servidores próprios hospedados em seu tabelionato.

O Colégio Notarial do Brasil recomenda aos notários analisarem a possibilidade de hospedar os seus sistemas em ambiente externo ao Tabelionato de Notas. A viabilidade de cada alternativa dependerá do porte do tabelionato, arquitetura dos sistemas em uso, infraestrutura da região e capacidade financeira. Não é certo que haverá redução de custos para o notário, mas esta solução provavelmente aumentará o nível de segurança de seu ambiente tecnológico. É uma tendência também existir ambientes híbridos nas empresas, sendo uma parcela de servidores próprios hospedados internamente e outra parcela em cloud. É uma questão de fazer contas e avaliar a melhor alternativa para o notário, considerando os riscos atuais de sua operação.

As alternativas sugeridas a serem avaliadas são:

• Ambiente cloud através de provedores conhecidos no mercado. O tabelião pagará a infraestrutura como serviço, não precisando investir em servidores próprios. Há serviços onde o sistema operacional e gerenciador de banco de dados é atualizado automaticamente pelo provedor, não sendo necessário ter equipes para manter o ambiente atualizado. Entretanto, deve-se ter cuidados com custos escondidos que nem sempre são visíveis no momento da contratação. Como premissa, o provedor a ser contratado deve ter Datacenters localizados no Brasil.

• Hospedar os servidores próprios do tabelionato em provedor externo. Também conhecido como serviço de Colocation, a vantagem neste modelo é que a infraestrutura da sala, segurança, redundância de energia elétrica e internet, é altamente avançada, com diversos fornecedores atendendo à classificação de mercado tier 3.

Para os casos de Datacenter próprio, recomenda-se ao notário adotar as seguintes medidas:

• Estabelecer sala exclusiva com acesso restrito, podendo ficar trancada com chave ou utilizar recursos de acesso através de autenticação forte, tais como, senha, biometria ou cartão magnético.

• No caso de acesso à sala através de autenticação forte, recomenda-se registrar todos os acessos e executar auditoria periódica
de acessos ao Datacenter pelos relatórios gerados por este sistema.

• O acesso de visitantes ou terceiros somente poderá ocorrer com acompanhamento de uma pessoa autorizada pelo notário.

• O Datacenter deve ser mantido limpo e organizado, não permitindo a entrada de nenhum tipo de alimento e bebida.

• Os computadores e outros equipamentos devem estar dispostos em armários adequados para este fim, de preferência em racks que podem ser trancados.

• O cabeamento atrás do rack deve estar disposto de forma organizada.

• A instalação elétrica deve ser adequada ao consumo dos equipamentos e ficar devidamente embutida, evitando fios à mostra que geram riscos de curtos ou interrupções de energia.

• **Infraestrutura de contingência:**

Recomenda-se também a elaboração de políticas de Contingência de forma a garantir que muitos dos problemas nos recursos tecnológicos não impactem a operação do tabelionato. O plano de prever as ações para os casos de falta de energia elétrica, falta de link de internet, pane no servidor, falha nos computadores e dispositivos utilizados pelos funcionários. Alguns dos principais pontos são:

• Backup

• Instalação de nobreak nos servidores e nas estações de atendimento (setor de firmas, procurações, certidões, financeiro, caixa etc.

• Estoque reserva de dispositivos

• Redundância: é a duplicação de componentes críticos do ambiente tecnológico, que em caso de falha do componente principal, o redundante é ativado sem prejudicar a operação do Tabelionato, garantindo a disponibilidade do serviço.

Sugere-se contratar os seguintes componentes redundantes:

• Link redundante: pode-se adotar estratégias de loadbalance, que distribui uniformemente a carga de trabalho entre os links contratados, e failover, que é um recurso que faz a transferência automática dos serviços do link principal para o redundante em caso de degradação do serviço do link principal.

• Servidores redundantes: servidores que ficam sincronizados com o principal e, neste caso, também pode-se adotar estratégias de load balance e failover.

• Fontes redundantes em servidores: é recomendado adquirir servidores com fontes redundantes, já que este componente também é passível de falhas.

Recomendações pelo perfil do Tabelionato de Notas

Visando adaptar as recomendações para o ambiente tecnológico dos Tabelionatos de Notas conforme o seu porte, apresentamos a seguir uma relação de itens considerados básicos para a operação. Como critério para a definição do porte do Tabelionato de Notas, foi considerado o número de funcionários, conforme faixas abaixo relacionadas:

- **Pequeno:** até 10 funcionários
- **Médio:** de 11 a 40 funcionários
- **Grande:** acima de 40 funcionários

A recomendação pode ser:

- **Opcional:** permite melhorias na operação, mas tem restrição pela complexidade ou alto grau de investimento para implementação.
- **Recomendável:** permite melhorias importantes na operação e há possibilidade de encontrar soluções adequadas ao porte do Tabelionato de Notas.

- **Obrigatório:** item essencial para a operação do Tabelionato de Notas.

Recomendação conforme o porte do Tabelionato de Notas			
Item	Pequeno	Médio	Grande
1. HARDWARE			
Computadores	Obrigatório	Obrigatório	Obrigatório
Impressoras	Obrigatório	Obrigatório	Obrigatório
Servidores	Recomendável	Obrigatório	Obrigatório
Roteador	Obrigatório[1]	Obrigatório[1]	Obrigatório[1]
Switch	Recomendável	Obrigatório	Obrigatório
Firewall por hardware	Opcional	Opcional	Recomendável
Nobreak para os servidores	Recomendável	Recomendável	Obrigatório
Nobreak para as estações	Recomendável	Recomendável	Recomendável
Leitores Biométricos	Recomendável	Recomendável	Obrigatório
Webcam	Recomendável	Recomendável	Obrigatório
Tablet para assinatura	Opcional	Opcional	Opcional
Biométrica			
2. SOFTWARE BÁSICO			
Sistema Operacional	Obrigatório	Obrigatório	Obrigatório
Serviço Diretório	Opcional	Recomendável	Obrigatório
Banco de Dados	Recomendável	Obrigatório	Obrigatório
Antivírus no Servidor	Recomendável	Recomendável	Obrigatório
Antivírus nas Estações	Obrigatório	Obrigatório	Obrigatório
Firewall por Software	Obrigatório	Obrigatório	Obrigatório
Software para Backup	Obrigatório	Obrigatório	Obrigatório
3. APLICATIVOS			
Sistema de Geração de Cartórios	Recomendável	Obrigatório	Obrigatório
Automação de Escritório	Obrigatório	Obrigatório	Obrigatório

Recomendação conforme o porte do Tabelionato de Notas			
Item	Pequeno	Médio	Grande
5. MECANISMOS DE PREVENÇÃO			
Backup Diário	Obrigatório	Obrigatório	Obrigatório
Backup Semanal Completo	Recomendado	Recomendado	Recomendado
Backup em Mídia Externa	Recomendado	Recomendado	Recomendado
Backup Remoto	Obrigatório	Obrigatório	Obrigatório
Utilização de Senhas Fortes	Recomendado	Recomendado	Recomendado
Atualização frequente de Antivírus	Obrigatório	Obrigatório	Obrigatório
Configuração de Firewall	Obrigatório	Obrigatório	Obrigatório
Software e Aplicativos originais	Obrigatório	Obrigatório	Obrigatório
Atualização frequente do Sistema Operacional e Aplicativos	Recomendado	Recomendado	Recomendado
Datacenter com sala fechada	Obrigatório	Obrigatório	Obrigatório
Acesso ao datacenter com biometria	Opcional	Opcional	Recomendado
Organização da fiação do datacenter	Recomendado	Recomendado	Recomendado
Navegação consciente da Web e e-mail	Obrigatório	Obrigatório	Obrigatório
Termos de Responsabilidade e de uso de equipamentos	Recomendado	Recomendado	Recomendado

Recomendação conforme o porte do Tabelionato de Notas			
Item	Pequeno	Médio	Grande
4. SERVIÇOS DE TERCEIROS			
Link de Internet	Obrigatório	Obrigatório	Obrigatório
Backup Remoto	Recomendado	Recomendado	Recomendado
Colocation	Recomendável	Recomendável	Recomendável
Servidor Cloud	Recomendável	Recomendável	Recomendável
Certificado SSL para sites com apenas páginas estáticas	Recomendado	Recomendado	Recomendado
Certificado SSL para sites com páginas dinâmicas	Recomendado	Obrigatório	Obrigatório
Senha segura para área restrita do site (função de administrador)	Obrigatório	Obrigatório	Obrigatório
Captcha nas consultas para evitar robôs de consulta	Recomendado	Recomendado	Recomendado
6. CONEXÃO À INTERNET			
Oferecer o serviço de acesso à internet aos clientes	Recomendado	Recomendado	Recomendado
O acesso à internet pelos clientes deve ocorrer em rede específica e exclusivamente para este fim	Obrigatório	Obrigatório	Obrigatório
Trocar a senha de acesso por clientes periodicamente	Obrigatório	Obrigatório	Obrigatório
Registar os históricos de acesso	Recomendável	Recomendável	Recomendável

[1] em geral, são fornecidos pelos provedores de Internet

Anexo 1 – Termo de Responsabilidade e Sigilo

O termo de responsabilidade e sigilo deverá ser assinado por todos os colaboradores do tabelionato de notas e comunicado na fase de contratação, a fim de mitigar possíveis riscos. Os funcionários já contratados devem assinar como anexo ao contrato de trabalho. Abaixo segue uma sugestão de conteúdo.

TERMO DE RESPONSABILIDADE E SIGILO

Nome: <nome> RG: _____

Eu, <nome> pelo presente instrumento, na condição de <função> do <nome do Tabelionato de Notas>, a seguir denominado <denominação>, comprometo-me a cumprir todas as orientações e determinações a seguir especificadas e outras editadas, em função do vínculo jurídico e funcional que tenho ou terei com o
<denominação>, bem como com as informações pertencentes ao <denominação>, ou por ele custodiadas, em razão da permissão de acesso aos recursos necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável que:

• Devo obedecer, cumprir e respeitar, as políticas, diretrizes, normas e procedimentos de Segurança da Informação do <denominação>, publicadas e armazenadas nos meios de comunicação internos que regem o uso dos recursos a mim disponibilizados, sejam estes digitais ou impressos; bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades profissionais.

• Qualquer meio de acesso a informações ou instalações, como identificador de usuário (USERID), senhas de acesso a sistemas (PASSWORD), aplicativos, internet, intranet, conta para acesso a correio eletrônico, crachás, cartões, chaves, tokens ou afins, que o <denominação> me forneceu ou vier a me fornecer são individuais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades funcionais perante a Instituição, devendo ser por mim devolvidos ou disponibilizados para o <denominação> em caso de exoneração, desligamento ou mudança de função.

• Meus acessos à internet e à conta de correio eletrônico por meio dos recursos do <denominação> devem ser utilizados única e exclusivamente para a realização de atividades ligadas privativamente às atividades do <denominação> e vinculadas às minhas atribuições.
• Todos os meus acessos efetuados e informações por mim manipuladas (sistemas de informação, correspondências, cartas, e-mails etc.), serão passíveis de verificação pelos representantes do <denominação>, que recebam atribuição para tal, a qualquer momento, independente de aviso prévio. Em decorrência disto, estou ciente que o
<denominação> é o legítimo proprietário e custo diante de todos os equipamentos, infraestrutura e sistemas de informação que serão por mim utilizados.
• As informações por mim geradas ou recebidas durante minha jornada de trabalho, desenvolvimento de atividades para o <denominação> ou em função desta, deverão tratar apenas de assuntos profissionais e ligados exclusivamente ao exercício de minha função.
• Não devo adquirir, reproduzir, instalar, utilizar ou distribuir cópias não autorizadas de softwares ou programas aplicativos, produtos, mesmo aqueles desenvolvidos internamente pelos departamentos técnicos pertencentes ao <denominação>.
• Não é permitida a entrada ou saída de informações do <denominação>, quer estas sejam em meios magnéticos (discos rígidos, cd's, fitas, pen drives, disquetes, dentre outros) ou em meios físicos (papel etc.) sem o conhecimento e autorização de seu responsável.

• Todos os recursos de tecnologia da informação a mim disponibilizados são para fins relacionados única e exclusivamente às minhas atividades profissionais, assim sendo, é expressamente proibido o uso destes recursos para outros fins.
• Em caso de utilização de acesso remoto, devidamente autorizado, aos recursos do
<denominação> para a execução de minhas atividades profissionais, devo manusear as informações obedecendo aos mesmos critérios de segurança exigidos nas instalações internas para o desempenho de minha função.
• Devo zelar pela segurança, pelo uso correto e pela manutenção adequada dos equipamentos existentes no âmbito corporativo compreendendo entre outros aspectos:
• Nunca deixar equipamento de minha utilização ativo sem antes bloquear seu acesso ou desativar a senha;
• Jamais emprestar minha senha ou utilizar a senha de outros;
• Solicitar eliminação ou bloqueio de minha senha ao ausentar-me por período longo;
• Nunca utilizar senhas triviais que possam ser facilmente descobertas;
• Não divulgar informações do <denominação>, ou de qualquer dado relativo aos clientes do <denominação>, a quem quer que seja sem a devida autorização de superiores hierárquicos;
• Não deixar relatórios, disquetes, cd's, ou quaisquer mídias com informações confidenciais em cima das mesas ou em local de fácil acesso;
• Não utilizar recursos ou equipamentos particulares no âmbito das instalações do
<denominação> para a realização de qualquer tipo de atividade, seja ela profissional ou não;
• Não utilizar software que não tenha sido devidamente homologado pelo departamento responsável;
• Respeitar as leis de direitos autorais e propriedade intelectual;
• Zelar pelos equipamentos pertencentes ao <denominação> a mim confiados para a execução de minhas atividades profissionais;
• Ao término do expediente, ou no caso de ausência prolongada, me comprometo a deixar meu local de trabalho limpo e organizado;

• Devo efetuar o descarte das informações de forma a impedir o seu resgate, independentemente do meio de armazenamento na qual a informação se encontra.
• Informar imediatamente ao superior ou à área competente do <denominação> acerca de qualquer violação das regras de sigilo.
• Responder mensagens eletrônicas de clientes no prazo máximo de 24 horas úteis, vedado o uso de mensagens automáticas.
• Reconheço que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser consideradas e mantidas em segredo, e que em caso de dúvida acerca da confidencialidade de determinada informação devo tratar a mesma sob sigilo até que venha a ser autorizado a tratá- la diferentemente pelo órgão responsável. Em hipótese alguma irei interpretar o silêncio do <denominação> como liberação de qualquer dos compromissos ora assumidos.
• Descumprindo os compromissos por mim assumidos neste termo estarei sujeito às sanções disciplinares aplicáveis.

<cidade>, xx de xx de xxxx.

_____
Assinatura

Anexo 2 – Termo de Uso para Acesso Remoto

O termo de uso para acesso remoto deverá ser assinado por todos que precisam efetuar algum tipo de acesso remoto ao ambiente tecnológico do Tabelionato de Notas, independentemente de onde esteja localizado. Este termo é válido para colaboradores e fornecedores contratados. Abaixo segue uma sugestão de conteúdo.

TERMO DE USO PARA ACESSO REMOTO A REDE DO <nome do Tabelionato de Notas>

DEVERES DO USUÁRIO:

• Permitir acesso da equipe de TI do <nome do Tabelionato de Notas> ou da prestadora de serviços ao computador sempre que se fizer necessário, para averiguação de segurança ou para configuração e/ou instalação de softwares que sejam essenciais à conexão com a rede.

• Ser responsável pela gestão de segurança de seu equipamento (emissão e recebimento de e-mails, acessos a sites, atualização de antivírus, anormalidades devem ser avisados a equipe de TI, etc).

• Ser responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo equipamento caracterizado acima;

• Ser responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo uso de seu login e senha em qualquer terminal da rede, através de uso próprio ou de terceiros;

• Utilizar-se do acesso apenas para atividades profissionais ligadas à atividade notarial;

• Ser responsável pelo licenciamento de software (sistema operacional e programas) instalado em seu equipamento. Comunicar à equipe de TI a instalação de qualquer aplicativo diverso daquele previamente configurado pelo Tabelionato.

• Informar à equipe de TI do <nome do Tabelionato> sobre alterações do Hardware do equipamento cadastrado ou sobre desconfiança de incidentes.

PROIBIÇÕES

• É proibida a transferência do direito de uso da rede do <nome do Tabelionato> a terceiros;

• É proibido o uso da rede para download de material que fira as leis de direitos autorais e propriedade intelectual (músicas, filmes, obras literárias, pesquisas científicas);

• É proibido o uso de serviços P2P (Peer-to-peer), tais como Kazza, Emule, torrent, ou quaisquer mecanismos de download similares, ainda que para executar download de arquivos que não firam direitos autorais;

• É proibido o acesso a conteúdo que promova o racismo, a contravenção, o preconceito, a pedofilia, e outros que sejam ilegais.

• Sendo o equipamento de propriedade do usuário, este não receberá qualquer tipo de suporte pela equipe de TI do <nome do Tabelionato de Notas>, exceto os relacionados ao acesso ao sistema.

PUNIÇÕES

Item único - O descumprimento de um dos deveres configurará falta grave e dará ensejo ao adequado procedimento disciplinar podendo, inclusive, motivar a pena de demissão.

OBSERVAÇÕES GERAIS

• A Gestão da infraestrutura da rede de dados responsabilidade da equipe de TI do

<nome do Tabelionato de Notas>. O serviço pede ser desativado a qualquer tempo, sem aviso prévio, por problemas lógicos ou elétricos, para manutenção ou garantia de segurança;

• A equipe de TI do <nome do Tabelionato de Notas> não tem responsabilidade sobre a instalação ou configuração de softwares nas máquinas do usuário cujas licenças pertençam à terceiros ou que ainda que gratuitos, não tenha relação com o uso da rede.

Cliente
<cidade>, xx de xx de xxxx.

_____
Assinatura

Anexo 3 – Termo de Uso sobre Computador Portátil e outros dispositivos

O termo de sobre computador portátil e outros dispositivos deverá ser assinado por todos que recebem um notebook e outros dispositivos para realizar suas atividades notariais no Tabelionato de Notas. Abaixo segue uma sugestão de conteúdo.

TERMO DE USO SOBRE COMPUTADOR PORTÁTIL (NOTEBOOK) E OUTROS DISPOSITIVOS DE PROPRIEDADE DO <nome do Tabelionato de Notas>

Identificação do Usuário: Nome: CPF.:
MAC da Placa wireless:
Modelo da Placa:
Modelo do Computador:
Fabricante:
Definições:
Rede lógica do <nome do Tabelionato de Notas> ou REDE: conjunto de equipamentos que prove comunicação entre computadores e acesso à internet de propriedade ou responsabilidade do <nome do Tabelionato de Notas>; Compreende, para o usuário final, a rede cabeada (pontos de rede fixos) e a rede sem fio.
USUÁRIO: funcionário vinculado ao <nome do Tabelionato de Notas>;
LOGIN: nome (ou número) com que o usuário identificar-se-á ao acessar a rede e/ou sistemas do <nome do Tabelionato de Notas>;
EQUIPAMENTO: computador pessoal, notebook ou outro dispositivo capaz de conectar- se à rede, de propriedade do usuário;

DIREITOS
01. O usuário poderá transportar o computador portátil e outros dispositivos para uso notarial fora do <nome do Tabelionato de Notas>.

DEVERES DO USUÁRIO:

• Permitir acesso da equipe de TI do <nome do Tabelionato de Notas> ou da prestadora de serviços ao computador e aos outros dispositivos sempre que se fizer necessário, para averiguação de segurança ou para configuração e/ou instalação de softwares que sejam essenciais à conexão com a rede.
• Ser responsável pela gestão de segurança de seu equipamento (instalação e atualização de antivírus, firewall, emissão e recebimento de e-mails, realização de cópias de segurança, compartilhamento de arquivos e pastas, dentre outras);
• Ser responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo equipamento caracterizado acima;
• Ser responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo uso de seu login e senha em qualquer terminal da rede, através de uso próprio ou de terceiros;
• Utilizar-se do acesso apenas para atividades profissionais ligadas à atividade notarial;
• Ser responsável pelo licenciamento de software (sistema operacional e programas) instalado em seu equipamento;
• Informar à equipe de TI do <nome do Tabelionato de Notas> ou da prestadora de serviços sobre alterações do Hardware do equipamento cadastrado ou sobre desconfiança de incidentes;

PROIBIÇÕES

• É proibida a transferência do direito de uso da rede do <nome do Tabelionato de Notas> a terceiros;
• É proibido o uso da rede para download de material que fira as leis de direitos autorais e propriedade intelectual (Musicas, Filmes, obras literárias, pesquisas científicas);
• É proibido o uso de serviços P2P (Peer-to-peer) ou quaisquer mecanismos de download similares, ainda que para executar download de arquivos que não firam direitos autorais;
• É proibido acesso a conteúdo que promova o racismo, a contravenção, o preconceito, a pedofilia, e outros que sejam ilegais.

PUNIÇÕES

• O descumprimento de um dos deveres levará à (1ª ocorrência) advertência por escrito, (2ª ocorrência) suspensão por 30 dias do uso da rede, (3ª ocorrência) suspensão definitiva do uso da rede;

• A realização de uma das proibições levará à (1a ocorrência) suspensão por 30 dias do uso da rede, (2a ocorrência) suspensão em caráter definitivo do uso da rede;

• Em caso de: acesso ou tentativa de acesso não autorizado à rede; acesso ou tentativa de acesso aos sistemas de gestão do <nome do Tabelionato de Notas>; dano ou tentativa de dano à imagem e às informações do <nome do Tabelionato de Notas>; uso da rede para ações ilícitas ou que prejudiquem terceiros; presença de vírus ou outros artifícios potencialmente danosos à rede e a outros usuários; ocorrerá imediata suspensão do direito de uso e constatado o dano, um relatório será encaminhado às instâncias devidas para que as penas sejam dimensionadas e aplicadas.

OBSERVAÇÕES GERAIS

• A Gestão da infraestrutura de rede <nome do Tabelionato de Notas> é da responsabilidade da equipe de TI do <nome do Tabelionato de Notas> ou da prestadora de serviços. O serviço pode ser desativado a qualquer tempo, sem aviso prévio, por problemas lógicos ou elétricos, para manutenção ou garantia de segurança;

• A equipe de TI do <nome do Tabelionato de Notas> ou da prestadora de serviços não tem responsabilidade sobre a instalação ou configuração de softwares nas máquinas do usuário cujas licenças pertençam à terceiros ou que ainda que gratuitos, não tenha relação com o uso da rede;

Estando ciente e tendo compreendido o quanto aqui se contém, assino sem restrições os deveres, proibições, punições e observações gerais.

<cidade>,_____de_____de_____.

Nome/Funcionário

Colégio Notarial do Brasil
CONSELHO FEDERAL

Manual de Boas Práticas do Ambiente Tecnológico do Notariado

Versão 1.0

Caso tenha alguma pergunta, dúvida ou sugestão de tecnologia, sinta-se à vontade para nos acionar através do:

Celular: (11) 95070-5615

WhatsApp: (11) 99617-2308

e-mail: duvidastec@notariado.org.br

Colégio Notarial do Brasil
CONSELHO FEDERAL