2º SERVIÇO DE REGISTRO CIVIL DAS PESSOAS NATURAIS E 6º TABELIONATO DE NOTAS DE MARINGÁ – ESTADO DO PARANÁ

OFICIAL MARIA REGINA PEREIRA BOEIRA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Em atendimento à Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, bem como ao Provimento n. 74/2018 do Conselho Nacional de Justiça – CNJ, o **2º SERVIÇO DE REGISTRO CIVIL DAS PESSOAS NATURAIS E 6º TABELIONATO DE NOTAS DE MARINGÁ – ESTADO DO PARANÁ**, por meio do presente instrumento, implementa a presente Política de Segurança da Informação.

O presente documento estabelece padrão de segurança da informação, no sentido de orientar seus colaboradores a utilizar os canais de comunicação, sistemas informatizados, computadores e demais instrumentos de trabalho, assim como a utilização de aparelhos pessoais dentro da perspectiva de proteção de dados pessoais. Trata-se de medida apta a adequar aos princípios e diretrizes definidas pela LGPD e normas correlatas, tendo por escopo respeitar a política institucional do **SERVIÇO REGISTRAL E NOTARIAL** e as regras de segurança da informação, consubstanciadas na segurança, integridade e disponibilidade de dados pessoais.

1. DIRETRIZES GERAIS

1.1. DEFINIÇÕES

Para melhor compreensão do presente documento, definem-se os seguintes termos:

a. **Serviço Registral**: corresponde ao 2º Serviço de Registro Civil das Pessoas Naturais e o 6º Tabelionato de Notas de Maringá – Estado do Paraná.

b. **Usuário**: toda e qualquer pessoa que exerça vínculo profissional ou de estágio junto ao 2º Serviço de Registro Civil das Pessoas Naturais e 6º Tabelionato de Notas de Maringá – Estado do Paraná.

c. **E-mail corporativo**: sistema de correio eletrônico cujo domínio identifica o **SERVIÇO REGISTRAL E NOTARIAL** e por meio do qual são exaradas comunicações oficiais. Ex.: exemplo@cartorio.com.br.

d. **Rede Social institucional**: mecanismos de comunicação de mensagens instantâneas como WhatsApp, Telegram, Instagram, Facebook, Messenger, dentre outros similares.

e. **Sistema informatizado**: dispositivo virtual capaz de receber, guardar, processar e disponibilizar informação de forma organizada para os fins programados.

f. **Aparelho pessoal**: dispositivo eletrônico de uso pessoal que permite a coleta, armazenamento, processamento, disseminação e eliminação de informação.

g. **Computador**: dispositivo eletrônico de uso profissional que permite acesso e controle de sistemas informatizados para fins de gestão e tratamento de dados pessoais.

h. **Recurso**: todo o meio direto ou indireto utilizado para o tratamento de dados pessoais, o que inclui a sua coleta, o seu trânsito interno e o armazenamento ou retenção do dado.

i. **Dado pessoal**: informação relacionada a pessoa natural identificada ou identificável (art. 5º, inciso I, da Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais).

j. **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 (art. 5º, inciso II, da Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais).

k. **Credencial de Acesso**: dispositivo virtual que identifica e define as permissões de acesso de um usuário em um ou mais sistemas ou qualquer tipo de recurso. É composta por uma sequência de caracteres (palavra de identificação) muitas vezes relacionada ao nome do usuário e uma senha. Uma credencial é válida quando criada por pessoa devidamente designada para esta função a de mais deve ser secreta, ou seja, apenas o titular da credencial pode conhecer a senha. O usuário titular da credencial é o responsável por mantê-la válida.

1.2. CAMPO DE APLICAÇÃO

Esta política se aplica a todos os colaboradores ou qualquer pessoa titular de uma ou mais credenciais de acesso aos recursos do **SERVIÇO REGISTRAL E NOTARIAL**, os quais deverão obrigatoriamente observar seus princípios, orientações e regras de

conduta, a fim de garantir o uso responsável da informação no exercício de suas funções profissionais.

1.3. OBJETIVO

A presente Política de Segurança da Informação visa respaldar o tratamento de dados pessoais e informações sensíveis custodiadas no âmbito da execução das atividades do **SERVIÇO REGISTRAL E NOTARIAL**, provendo orientações de uso, definindo regras e comportamentos, bem como para vedar o uso indevido das respectivas ferramentas de comunicação por aparelhos pessoais.

2. DIRETRIZES PARA A SEGURANÇA DA INFORMAÇÃO

2.1. PRIVACIDADE

a. Os e-mails corporativos, sistemas informatizados e as redes sociais institucionais são disponibilizados aos usuários como ferramenta de trabalho e, portanto, são de titularidade do **SERVIÇO REGISTRAL E NOTARIAL** e somente devem ser utilizados dentro do seu escopo de trabalho;

b. O uso de e-mail ou de outros recursos de mensagens instantâneas por redes sociais deverá atender linguagem compatível com o ambiente de trabalho e adequado à finalidade pela qual foi instituído;

c. As mensagens deverão ser retidas quando tiverem importância para instrução de procedimentos internos e eliminadas quando houver o adequado registro da informação nos procedimentos afetos à Lei de Registros Públicos ou normas correlatas;

d. O **SERVIÇO REGISTRAL E NOTARIAL**, na qualidade de titular do sistema de e-mail corporativo, de sistemas informatizados ou das redes sociais institucionais ou outro recurso computacional, poderá, a qualquer tempo e sem aviso prévio, monitorar o uso do sistema e o conteúdo das mensagens quando julgar necessário;

e. Nas situações pertinentes, em que se verifique a necessidade de quebra de sigilo de e-mail, o **SERVIÇO REGISTRAL E NOTARIAL** observará os cuidados relativos à proteção do conteúdo dentro da perspectiva de proteção de dados pessoais.

2.2. FINALIDADE

O serviço de e-mail corporativo ou de redes sociais institucionais tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções desempenhadas pelo **SERVIÇO REGISTRAL E NOTARIAL**.

2.3. CRIAÇÃO DE CONTAS DE E-MAIL

A concessão de contas de e-mail corporativo é franqueada aos colaboradores a critério da administração do **SERVIÇO REGISTRAL E NOTARIAL**, que sempre levará em conta os critérios de necessidade e finalidade em relação à atividade por ele desempenhada.

Assim que criado o e-mail será enviado ao usuário sua credencial de acesso com senha provisória e a presente Política de Segurança da Informação.

2.4. SISTEMAS INFORMATIZADOS

O acesso aos sistemas informatizados será franqueado aos usuários do **SERVIÇO REGISTRAL E NOTARIAL** de acordo com a função profissional e a atividade desempenhada de cada colaborador, a critério da administração do **SERVIÇO REGISTRAL E NOTARIAL**, que sempre levará em conta os parâmetros de necessidade e finalidade.

Uma vez criada uma credencial de acesso será encaminhada ao respectivo usuário em seu e-mail institucional, cabendo a este validar a sua credencial relacionado a ela uma senha secreta.

2.5. RESPONSABILIDADE

O usuário é responsável por:

a. Conteúdo das mensagens enviadas via e-mail corporativo sob sua identificação, ou então, pelas redes sociais institucionais que tenha acesso;

b. Proteger a confidencialidade de sua senha de acesso a computadores e sistemas informatizados – elas não poderão ser compartilhadas, sendo de uso pessoal e intransferível. O uso de credencial inválida é um incidente de segurança e denota falta grave;

c. Realizar periodicamente a troca de suas senhas, pelo que se recomenda seja feito trienalmente ou quando solicitado pelo encarregado da segurança da informação;

d. O usuário deverá revisar as mensagens de e-mail ou de redes sociais suscetíveis de eliminação com periodicidade mínima mensal;

e. Verificar se a origem de mensagens recebidas é de fonte confiável e de interesse do **SERVIÇO REGISTRAL E NOTARIAL**, a fim de evitar algum dano aos recursos tecnológicos como vírus, *malware*, dentre outras hipóteses de vulnerabilidade;

f. O acesso aos computadores é restrito, portanto, os colaboradores deverão sempre desativar o *login* de seu computador quando se ausentar da estação de trabalho, bem como zelar com aplicativos e acessos a sites não autorizados ou que vulnerem a segurança do ambiente corporativo;

g. Não emprestar login e senha para quaisquer pessoas;

h. Os colaboradores não poderão deixar documentos que contenham dados pessoais expostos sobre a mesa ou em locais visíveis quando não houver necessidade. Em se tratando de documento físico deverão ser guardados em pastas organizadas, a fim de que se auxilie a eficiência do serviço;

i. Ao enviar mensagens eletrônicas, sempre conferir a correção do endereço destinatário, bem como a autenticidade da identificação do interlocutor, certificando que o endereço levará a mensagem de fato a quem deve tomar conhecimento do conteúdo;

j. Não abrir *spams* e desconfiar de mensagens que fujam ao padrão de rotina, uma vez que podem conter vírus e comprometer a segurança dos computadores e sistemas informatizados. Acaso tais mensagens sejam recebidas, dever-se-á bloquear o remetente e eliminar a mensagem;

k. Comunicar ao superior hierárquico qualquer suspeita de incidente de segurança da informação;

l. Os colaboradores deverão evitar a utilização de aparelhos pessoais para rotinas operacionais que possam ser resolvidas por e-mail, por sistema informatizado ou por aparelho institucional. Tal uso somente se justificará em hipóteses de estrita urgência e necessidade;

m. Caso seja utilizado aparelho pessoal, uma vez sanada a urgência mediante a recepção dos dados dentro dos padrões operacionais de trabalho, as informações deverão ser eliminadas do mesmo tão logo seja possível, sendo

vedado o uso do dispositivo pessoal como repositório de dados do **SERVIÇO REGISTRAL E NOTARIAL** ou a ela custodiado;

n. Os colaboradores deverão evitar/cuidar com a utilização de jogos e aplicativos no seu aparelho pessoal, pois podem se tratar de porta de entrada para eventos indesejados e incidentes de segurança;

o. Os colaboradores não podem usar os recursos do **SERVIÇO REGISTRAL E NOTARIAL** para qualquer finalidade que não seja a execução de sua rotina de trabalho;

p. É falta grave instalar qualquer tipo de programa nos computadores ou alterar a configuração de qualquer recurso de que tenha acesso.

Eventuais práticas indevidas realizadas por meio de sistemas informatizados, e-mail corporativo ou de redes sociais de caráter institucional, que violem a presente Política, bem qualquer outra norma interna ensejará na responsabilização, a depender da gravidade da conduta e da extensão dos danos causados.

2.6. BOAS PRÁTICAS DE USO

Ao enviar ou responder uma mensagem para um destinatário com cópia para várias pessoas, tenha certeza de que todas as pessoas realmente devem receber a mensagem.
Lembre-se que a facilidade de se copiar uma mensagem no e-mail corporativo pode nos levar a endereçar cópias para muitas pessoas, porém, cópias desnecessárias sobrecarregam os recursos tecnológicos e podem representar compartilhamento desnecessário ou desproporcional.

Em caso de troca de mensagens que envolvam conteúdo confidencial do cidadão, colaborador ou terceiro, deve-se evitar ao máximo o envio/compartilhamento de tais dados pelas vias eletrônicas, excetuando-se situações de justificada urgência. Caso seja praticada dessa forma, tão logo seja sanada excepcionalidade, deverá promover cuidadosamente ao rastreio de dados para o adequado tratamento conforme as regras internas de segurança, promovendo-se a eliminação do dado.

Mensagens contendo texto ou imagem não profissional, de propaganda, ou então, de origem duvidosa, não deverão ser encaminhadas, reproduzidas ou respondidas. Essa hipótese abrange, inclusive, a solicitação de cancelamento do envio de *spam*, como por exemplo: "*Clique Aqui caso não queira mais receber este e-mail*".

Recomenda-se a exclusão periódica de e-mails desnecessários, inclusive e-mails da lixeira e da pasta de mensagens enviadas, a fim de não sobrecarregar os recursos

tecnológicos e não vulnerar a política de proteção de dados pessoais em caso de ataques ou acessos indevidos.

Por fim, ao enviar e-mails acompanhados de arquivos anexos, certifique-se de que os tamanhos da mensagem e dos arquivos não ultrapassam o limite de envio por e-mail e com quem ele está sendo compartilhado.

2.7. GRUPOS INTERNOS DE WHATSAPP

Os colaboradores poderão participar de grupos de WhatsApp (e similares) instituídos pelo **SERVIÇO REGISTRAL E NOTARIAL**, sempre com observância das regras abaixo estipuladas:

a. Apenas os gestores do **SERVIÇO REGISTRAL E NOTARIAL** podem criar e administrar grupos de interesse pertinentes ao trabalho.

b. A participação do colaborador em grupos de *WhatsApp* é voluntária. O colaborador que não aceitar participar de grupos de *WhatsApp* em prol dos trabalhos não será repreendido ou penalizado;

c. Os colaboradores que aceitarem participar dos grupos de *WhatsApp* utilizarão os próprios celulares para tal finalidade. Quando aceitar participar dos grupos também aceitará utilizar o celular de sua propriedade e uso particular.

d. Os grupos de *WhatsApp* criados institucionalmente devem ser utilizados unicamente em benefício das funções exercidas pelos colaboradores.

e. Cabe somente à supervisão a decisão pela utilização de grupos de *WhatsApp*, bem como a criação e administração desses grupos.

f. Compete ao gestor disciplinar regras sobre as informações que podem ser veiculadas no grupo, o tempo de armazenamento e prestar orientações aos colaboradores para garantir a segurança da informação e evitar, sempre que possível, relacionar dados ou questões pessoais, sejam eles relacionados à equipe ou terceiros;

g. A Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018), que protege os dados pessoais de todas as pessoas físicas, impõe a obrigação de estrito cuidado com as informações, sobretudo daquelas que individualizam a pessoa (nome, RG, CPF, estado civil, endereço, sexo, religião, etc.). Aqueles que infringirem as obrigações dessa lei estão sujeitos a multas e processos.

h. Todos os participantes dos grupos devem ficar muito atentos para o que e a quem transmitem informações. Os dados dos usuários do **SERVIÇO REGISTRAL E NOTARIAL** são sigilosos e devem ser utilizados pelos colaboradores somente para o exercício das suas atividades específicas. Permite-se o compartilhamento desses dados exclusivamente com os demais colaboradores envolvidos nessas atividades e dentro da sua finalidade. Tais informações JAMAIS poderão ser transmitidas a terceiros pelos colaboradores de forma direta ou indireta sem que ocorram pelos meios previstos em lei (ex. certidão).

i. Os participantes não devem mencionar dados sigilosos nos grupos de *WhatsApp*, seja de colaboradores internos e, principalmente, de seus usuários.

j. As mensagens trocadas por meio do *WhatsApp* do trabalho não devem ser compartilhadas com terceiros, independentemente do seu teor ou relevância. Muitas vezes frases soltas ou fora de seu contexto tomam uma relevância além do esperado e podem se transformar em situações desagradáveis.

k. A utilização dos grupos de *WhatsApp* pelos colaboradores deve ocorrer nos horários de expediente não sendo permitida mensagens de trabalho em grupos coletivos fora dos horários convencionados.

l. Os colaboradores que aderirem à participação nos grupos de *WhatsApp* não são obrigados a receber e responder as mensagens fora do horário de trabalho, em fins de semana, feriados ou férias.

m. Se o colaborador receber mensagens fora do horário de trabalho deve ignorá-las e somente visualizá-las no próximo turno de trabalho.

n. Ainda que esteja em horário de trabalho, o colaborador não deve prejudicar suas rotinas para a visualização e atendimento/resposta das mensagens que receber, devendo priorizar os trabalhos presenciais do seu cargo e atender as diretivas de trabalho repassadas em documento físico ou e-mail. A presente orientação apenas é excepcionada quando tratar-se de atendimento de *WhatsApp* institucional e dentro das atribuições profissionais designadas pelo Oficial ou preposto expressamente designado.

o. Os grupos de *WhatsApp* somente podem veicular matérias/assuntos relacionados aos trabalhos realizados pela equipe, devendo os colaboradores evitar outros assuntos ou vinculação de "memes", vídeos, charges, piadas, dentre outros.

p. O colaborador deve ser objetivo, preciso e muito cuidadoso com o uso de abreviações e emoticons. As famosas "carinhas" podem ser interpretadas de forma errada e gerar mal-entendidos.

q. Os colaboradores não podem utilizar os grupos de *WhatsApp* para incitar discórdia ou proferir palavras de baixo calão, ou ainda fazer menção sobre a vida pessoal dos demais colaboradores, sendo proibidas conversas inadequadas ou que denotem convicções pessoais sem pertinência com o contexto das funções ou das mensagens.

r. O **SERVIÇO REGISTRAL E NOTARIAL**, a qualquer tempo, pode ter acesso às conversas registradas nos grupos de WhatsApp criados para a execução dos trabalhos.

s. Espera-se dos colaboradores atitudes responsáveis, tolerantes e respeitosas no uso dos grupos de *WhatsApp.*

t. Os colaboradores têm responsabilidade funcional e pessoal sobre o que postam nos grupos de *WhatsApp*. Os superiores hierárquicos, tomando conhecimento do uso inadequado desses grupos, poderão aplicar penalidades aos colaboradores, inclusive de demissão, a depender do grau da infração e sua caracterização em lei.

u. Os grupos de *WhatsApp* não podem ser usados para a transmissão oficial de ordens ou diretivas de trabalho, que devem ser feitas preferencialmente via e-mail corporativo. O uso do aplicativo se limita a reiteração ou reforços de diretivas do **SERVIÇO REGISTRAL E NOTARIAL**.

v. Os gestores não podem utilizar os grupos de *WhatsApp* para aplicar penalidade de advertência, suspensão ou demissão a colaboradores.

w. Os colaboradores jamais poderão compartilhar com terceiros o conteúdo corporativo. Consideram-se terceiros as pessoas que estão fora do grupo de *WhatsApp* em que as informações foram inseridas.

x. Os colaboradores devem cuidar com suas habilitações de *backup* e adotar as ferramentas de segurança adequada nos seus aparelhos pessoais, a fim de evitar acesso indevido ao grupo ou vulneração das informações da instituição mantidas em aparelho particular.

2.8. VEDAÇÕES

O **SERVIÇO REGISTRAL E NOTARIAL** veda o uso de e-mails corporativos ou de redes sociais institucionais cujo objetivo seja o de:

a. Praticar crimes e infrações de qualquer natureza;

b. Expor cidadãos e seus familiares;

c. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

d. Disseminar vírus ou qualquer outro tipo de programa de computador nocivo ao ambiente de rede, que não seja destinado ao desempenho de suas funções;

e. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", bem como, e-mails de origem e conteúdo duvidoso;

f. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político partidário;

g. Enviar arquivos de áudio, vídeo ou animação, salvo os que tenham relação com as funções institucionais;

h. Divulgar, no todo ou em parte, endereços eletrônicos corporativos, salvo quando a indicação se mostrar necessária para o desempenho das atividades institucionais, com a devida autorização do titular do e-mail ou de seu superior hierárquico quando tratar-se de obrigação legal ou regulamentar;

i. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema ou a imagem fora das hipóteses normativas previstas para a atividade;

j. Reproduzir qualquer material recebido pelo e-mail corporativo ou outro meio que possa infringir direitos autorais, marcas, licença de software ou patentes existentes, sem que haja permissão comprovada do criador do trabalho;

k. Encaminhar mensagens que representem a opinião pessoal do titular do e-mail, apresentando-as em nome do **SERVIÇO REGISTRAL E NOTARIAL**;

l. Cadastrar o respectivo endereço de e-mail em sites de compras, em listas do tipo *Feed* e *News* (ex.: mercadolivre.com), pois ocasionam o recebimento de *Spams*, os quais podem ocasionar diversas intercorrências como bloqueio do

domínio para envio de mensagens e sobrecarga dos servidores, dentre outras vulnerabilidades;

m. Utilizar o e-mail, sistemas informatizados e redes sociais institucionais de forma não prevista nesta Política.