# 2º CARTÓRIO DE PROTESTO
# DE CAMPO GRANDE/MS

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
# (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD)

**2023**

# Sumário

## 1. Objetivos

Esta Política de Segurança da Informação apresenta as diretrizes que norteiam as normas e padrões para proteção da informação na serventia, com mecanismos preventivos de controle físico e lógico, com os objetivos de assegurar a proteção no tratamento de dados pessoais e a continuidade dos serviços prestados à população.

As diretrizes aqui trazidas deverão ser implementadas, monitoradas, analisadas criticamente sempre que necessário, bem como melhoradas continuamente, a fim de garantir o cumprimento dos objetivos de segurança da serventia.

Esta Política ficará disponível na sua integralidade e sempre em sua versão aprovada mais recente no site da serventia, bem como em cópia impressa junto ao Encarregado e foi formulada tendo como base os artigos 46 e seguintes da LGPD e princípios desta, além do artigo 12 do Provimento 134/2022 do CNJ e do Provimento 74/2018 também do CNJ.

Desde o ano de 2018, quando foram publicados a LGPD – Lei Geral de Proteção de Dados e o Provimento nº 74/2018, pelo CNJ, que dispõe sobre padrões mínimos de segurança da informação para as serventias extrajudiciais, os cartórios já têm o dever de adequar seus sistemas internos às exigências de segurança da informação.

É de responsabilidade da alta administração da serventia o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação.

Essa política se aplica a todos os colaboradores, fornecedores e prestadores de serviços que utilizem ou forneçam serviços tecnológicos relevantes.

## 2. Conceitos

Segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- Confidencialidade: garante que a informação seja acessível somente às pessoas autorizadas, pelo período necessário;

- Disponibilidade: garante que a informação esteja disponível às pessoas autorizadas, sempre que se faça necessário;

- Integridade: garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

## 3. Definições

- Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa natural. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição;

- Informação sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para a serventia e outras partas interessadas;

- Ativos de informação: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a organização e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento;

- Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela organização para suportar suas operações;

- Dados pessoais: informação relacionada a pessoa natural/física identificada ou identificável;

- Dados pessoais sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à 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;

- Grupo gestor da segurança da informação: grupo de apoio ao encarregado de dados pessoais, que deve ter um perfil multidisciplinar e contar com a participação de gestores de diferentes áreas da serventia, podendo, ainda, utilizar especialistas internos ou externos para apoiarem os assuntos que exijam conhecimento técnico específico.

## 4. Informação

### 4.1 Tratamento da informação

A informação, sobretudo os dados pessoais, sob custódia desta serventia está protegida contra o acesso de pessoas não autorizadas.

São usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário. A informação é armazenada pelo tempo determinado pela organização, legislação ou regulação vigente, o que for maior. O local de armazenamento das informações é apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

Em conformidade com o Provimento nº 74/2018 do CNJ, esta serventia conta com:

- plano de continuidade para eventuais incidentes de segurança, que atenda às normas de interoperabilidade, legibilidade e recuperação de informações (art. 2º, parágrafo único), bem como medidas que possibilitem a transmissão facilitada do acervo, em caso de sucessão (art. 7º).
- padrões mínimos de segurança e integridade para armazenamento de dados, com backups em nuvem e backups físicos de periodicidade máxima de 24 horas e hospedagem em local distinto da instalação da serventia (art. 3º).
- sistema escalas de permissões seccionados por função, associados a perfis individuais, cujo acesso deve ocorrer com dupla autenticação: por usuário e senha e por certificação digital ou biometria (art. 4º).

- trilhas de auditoria que permitem rastrear e identificar acessos ou modificações, as quais devem ser preservadas por backup (art. 5º).

Também, em conformidade com a classe desta serventia, atendemos o Provimento 74/2018 do CNJ no que concerne à adoção de tecnologias obrigatórias.

Por sua vez, atendendo à LGPD (artigos 46 a 49) e Provimento 134/2022 do CNJ, esta serventia adotou como critérios para a construção desta política de segurança da informação:

- medidas de segurança técnicas e organizacionais;
- previsão de adoção de mecanismos de segurança, desde a concepção de novos produtos os serviços (*security by design*);
- plano de resposta a incidentes;
- avaliação dos sistemas e banco de dados em que houver tratamento de dados pessoais e/ou tratamento de dados sensíveis, submetendo tais resultados à ciência do Encarregado pelo tratamento de dados pela serventia;
- avaliação da segurança de integrações de sistemas;
- análise de segurança das hipóteses de compartilhamento de dados pessoais com terceiros; e
- realização de treinamento.

## 4.2 Classificação da informação

A informação produzida no desenvolvimento das atividades da serventia foi classificada em conformidade com os níveis de confidencialidade abaixo:

Pública: informação que pode ser acessada pelos usuários, fornecedores, prestadores de serviços e público em geral.

Interna: informação que só pode ser acessada pelos colaboradores da serventia e que possuem um grau de confidencialidade que pode comprometer a proteção dos dados.

Confidencial: informação que pode ser acessada por usuários e por parceiros da serventia, especificamente autorizados. A divulgação não autorizada dessa informação pode causar impactos (financeiro, de imagem ou operacional) às atividades administrativas, notariais e registrais ou aos seus usuários.

Restrita: informação que pode ser acessada somente por usuário da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos legais e de imagem à serventia.

### 4.3 Acesso à informação

O acesso à informação é controlado através de procedimentos padronizados para a liberação e/ou exclusão dos acessos, conforme demandas dos processos operacionais internos. O acesso e o uso dos sistemas de informação, diretórios de rede, bancos de dados e demais recursos são restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Os colaboradores da serventia são totalmente responsáveis pela posse e utilização de suas senhas, bem como pelas ações daí decorrentes.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da área de suporte técnico ou por prestadores de serviço, é controlado e restrito aos serviços estritamente necessários, devendo ser mantidas trilhas de utilização.

### 4.4 Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco. As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da serventia.

Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em uso ou logado com a credencial do colaborador que necessita do suporte.

### 4.5 Sistemas e recursos de rede

Sistemas e recursos de rede desenvolvidos fora da serventia, de propriedade de terceiros (com licença de uso para a organização), devem ter a biblioteca de fontes e de recursos adicionais (bibliotecas adquiridas, componentes, etc.) sob custódia de uma entidade idônea, de comum acordo entre a organização e a empresa fornecedora do software. Tais fontes devem sempre ser atualizadas e verificadas quanto à sua validade e sincronização com a versão em uso no ambiente de operações.

É terminantemente proibido o uso de programas ilegais (software pirata). Os usuários não podem, em hipótese alguma, instalar este tipo de programa nos equipamentos da serventia. Periodicamente, o pessoal da área de suporte técnico interno ou prestador de serviço fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

## *5. Security by Design*

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o *Security by Design.* O que implica em ter a privacidade e a segurança dos dados pessoais como parte integrante das prioridades, projetos, objetivos, operações e planejamentos da serventia, segundo os seus princípios.

## 6. Plano de continuidade do negócio

O plano de continuidade de negócios desta serventia tem como meta garantir a disponibilidade do ambiente em caso de incidente. Esta serventia e seus responsáveis se mantêm continuamente atentos à identificação do que não pode parar, implementando ferramentas para que os serviços continuem funcionando mesmo após um incidente, de acordo com as normas de segurança e a privacidade dos dados pessoais.

O plano de continuidade deve ser revisado e atualizado com periodicidade definida, considerando sua realização pelo menos uma vez ao ano e/ou sempre que considerado necessário.

O plano de continuidade de negócios desta serventia já se encontra formulado nos exatos termos do art. 2º, parágrafo único, I e art. 7º, ambos do Provimento 74/2018 CNJ.

## 7. Responsabilidades

Cabe a todos os colaboradores e demais partes envolvidas:

- Cumprir fielmente políticas, normas e procedimentos de segurança da informação, incluindo regras estabelecidas neste documento;
- Buscar orientação do superior quando houver dúvidas relacionadas à segurança da informação;
- Assinar o Termo de Responsabilidade, formalizando a ciência da PSI e das normas de segurança da informação, bem como assumindo a responsabilidade pelo seu cumprimento;
- Proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela serventia e/ou titular;
- Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da instituição;
- Prezar pela segurança das informações confidenciais, incluindo todos e quaisquer dados pessoais a que tiverem acesso;
- Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manuseá-los, e em conformidade com as regras do Provimento 134/2022 do CNJ;
- Comunicar imediatamente ao encarregado do tratamento de dados pessoais qualquer incidente de segurança, descumprimento ou violação desta Política e/ou das demais normas e procedimentos aplicáveis;
- Comunicar imediatamente o encarregado de dados e o responsável pelo TI da serventia sobre qualquer suspeita de vírus ou problema na funcionalidade do equipamento usado, bem como identificação de dispositivos estranhos conectados ao equipamento.

Também é dever de todos

- Considerar a informação como sendo um ativo da serventia, como um recurso crítico e necessário para a realização dos trabalhos.
- É de responsabilidade do superior de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido

neste documento.

- Todo dispositivo da serventia de acesso aos seus sistemas deve sofrer bloqueio automático após 05 minutos de inatividade (computadores, celulares, smartphones, tablets ou qualquer outro dispositivo, móvel ou não).
- Bloquear o acesso ao computador sempre que sair da mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais guardados e seguros, quando não os estiver utilizando a fim de não expor desnecessariamente informações classificadas.
- Não instalar softwares não aprovados pelo responsável pela área de TI e segurança de informação e pelo Encarregado de dados em dispositivos que acessam os sistemas da serventia, em especial computadores, notebooks e dispositivos portáteis como tablets, celulares e smartphones.

## 8. Diretrizes gerais

### 8.1 Dados dos colaboradores

Entende-se por colaborador toda e qualquer pessoa física, contratada pela CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade na serventia.

A serventia se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores, além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de colaboradores serão considerados confidenciais.

### 8.2. Da área de recursos humanos

Cabe à gestão de Recursos Humanos colher e arquivar a assinatura do Termo de Responsabilidade e Ciência da Política e Normas de Segurança da Informação, tanto na fase de contratação dos funcionários, prestadores de serviços, estagiários e afins, quanto dos profissionais já contratados.

### 8.3 Identificação e autenticação

Todo usuário possui uma identidade e será identificado para cada plataforma de tecnologia que estiver autorizado a utilizar por:

- Um ID (login) de usuário não compartilhável;
- Senha única (estática) ou dinâmica, chave privada, dados biométricos ou outro mecanismo de autenticação.

Administração do acesso de usuários: cada gestor da informação é responsável por definir e manter atualizados os perfis de acesso visando o acesso mínimo necessário para a execução das atividades, bem como evitando conflitos de interesse.

### 8.3.1 Política de senhas

Um sistema efetivo de controle de acesso será utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes protegido por senhas;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);
- Os sistemas são programados para nunca exibir a senha na tela;
- As senhas são individuais e intransferíveis: são de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis;
- Os tipos de caracteres utilizados para a formação da senha consideram:
    1. Letras maiúsculas;
    2. Letras minúsculas;
    3. Números;
    4. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !).
- As senhas devem ter um tamanho mínimo de 08 (oito) caracteres, sendo obrigatória a utilização de, no mínimo, três dos quatro tipos de caracteres acima.

## 8.4 Arquivos de trabalho

Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento das operações, são mantidos nos servidores de arquivos, em sistema que permite o controle, comparação e gestão de diferentes versões.

O acesso ao SVN fora das dependências da serventia é bloqueado e proibido, salvo se realizado através de VPN, com a devida permissão do responsável pela serventia.

## 8.5 Arquivos individuais

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do serviço entregável pelo seu trabalho, seja ele interno ou para clientes. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas. A cópia de segurança destes arquivos é de responsabilidade dos próprios usuários.

## 8.6 Cópias de segurança, recuperação e integridade dos sistemas e de seus bancos de dados

É de responsabilidade do pessoal da área de suporte técnico interno ou prestadores de serviço de TI, manter e documentar os planos de backups e garantir a execução dos procedimentos definidos para tal, e que passam **a fazer parte desta política de segurança da informação, com a observação estrita ao Provimento 74/2018 do CNJ.**

## 8.7 Testes regulares de armazenamento e recuperação de dados

Todo e qualquer meio de armazenamento, assim como os procedimentos de recuperação, devem ser regularmente testados, garantindo sua efetividade. A periodicidade dos testes de segurança deve ser de, ao menos uma, a cada 24 horas, considerando o nível de risco do negócio. Devem ser mantidas evidências do sucesso dos testes feitos.

Deverão ser obedecidas e observadas todas as previsões do Provimento 74/2018 do CNJ acerca do assunto.

## 8.8. Uso da internet

A Internet abrange vários aspectos e serviços (websites de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades da serventia.

O acesso à Internet deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia. O usuário deve restringir o acesso aos websites ainda não bloqueados que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (Webmail, jogos, etc.). Deve também comunicar o endereço eletrônico desses websites à área de Segurança da Informação, que deverá realizar seu imediato bloqueio.

É proibido o acesso a redes sociais pessoais através dos equipamentos da serventia.

O acesso à Internet é realizado através de “servidores de acesso” protegidos por sistemas de Firewall. Quando for necessário o acesso utilizando uma segunda conexão através de modem ou rede wi-fi, a configuração da máquina deve garantir o isolamento da rede normal de serviço da serventia, evitando, assim, que uma contaminação seja propagada. Os requisitos de segurança dessas máquinas em particular, devem ser respeitados (antivírus e firewall local). Casos específicos como esses necessitam ser aprovados pelos responsáveis da área de segurança da informação.

## 8.9 Uso do correio eletrônico - (“e-mail”)

O correio eletrônico fornecido pela serventia é uma ferramenta de trabalho, uma tecnologia necessária para facilitar a comunicação interna, comunicação com clientes, usuários, fornecedores e outros grupos que tenham relação. É de responsabilidade do usuário a utilização da tecnologia de forma adequada e para fins estritamente profissional, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.

Em caso de congestionamento no sistema de correio eletrônico a área responsável da segurança da informação da serventia fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

## 9. Conscientização de segurança da informação

Um plano de conscientização da segurança da informação será executado para atingir o seguinte objetivo: “Garantir que a segurança da informação não seja apenas conhecida, mas compreendida por todos os colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de segurança de forma a atingir uma melhor utilização e proteção à informação”.

Todos os colaboradores serão treinados e orientados sobre a Política de Privacidade e a Política de Segurança da Informação desta serventia, que sempre estará disponível aos mesmos.

## 10. Da proteção de dados pessoais

Esta serventia, em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais e às boas práticas de segurança da informação, garante a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratada em conformidade com requisitos normativos internos e externos.

Dados extrajudiciais estão, ainda, sujeitos às disposições do Provimento nº 50/2015 do CNJ que dispõe sobre a conservação de documentos (Temporalidade), bem como sujeitam-se às disposições do Provimento nº 74/2018 do CNJ que trata sobre os requisitos de tecnologia da informação (Ativos de TI) das serventias extrajudiciais, normativas estas integralmente observadas e atendidas.

## 11. Do plano de respostas a incidentes

É de responsabilidade do Encarregado de Dados da Serventia elaborar e revisar, quando necessário, o plano de comunicação e resposta a incidentes cibernéticos que conterá cada etapa de cada tratativa a partir da identificação de um incidente.

A gestão de tratamento de incidentes de segurança da informação deverá sempre considerar o registro, a análise de causa e impacto, definição de papéis e responsabilidades, avaliação de relevância, monitoramento contínuo e o controle dos efeitos dos incidentes.

O Encarregado de dados deverá documentar todas as ocorrências de brechas de segurança que tomar conhecimento ou lhe for comunicada e colher todas as evidências possíveis quando identificar ou for noticiada violações intencionais, tomando as medidas para sanar as ocorrências.

## 12. Disposições finais

As infrações a esta PSI e às Normas de Segurança da Informação serão passíveis de processo disciplinar, podendo resultar de mera advertência até demissão por justa causa. A qualquer tempo, e em qualquer um dos casos previstos, prevalecendo o descumprimento das regras expostas, a serventia poderá bloquear temporariamente o acesso do usuário e comunicar os motivos ao profissional e ao gestor da área.

O uso de qualquer recurso da serventia para atividades ilegais é motivo de demissão por justa causa e a instituição vai cooperar ativamente com as autoridades.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna desta serventia.

Esta política deve ser revista e atualizada em intervalos não superiores a 2 (dois) anos, a fim de garantir que todos os requisitos de segurança técnicos e legais implementados sejam cumpridos e atualizados nos termos da legislação de regência, e entrará em vigor na presente data.

Campo Grande/MS, 10 de Fevereiro de 2023.

## Modelo de Termo de Responsabilidade:

Eu (Nome do Colaborador), código funcional Nº (número), CPF/MF Nº (número) declaro para os devidos fins e efeitos de direito que o Cartório trouxe ao meu conhecimento o conteúdo das diretrizes, violações, normas e responsabilidades que regem sua Política de Segurança de Informação, que ora declaro ter lido, estando ciente e responsável pelo que segue:

1. Qualquer meio de acesso às informações ou instalações (como identificações de usuário, senhas, crachás, cartões, chaves etc.) que a organização me forneceu ou vier a fornecer são pessoais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades perante o Cartório;

2. Todas as informações utilizadas no Cartório, sejam elas de sua propriedade, de clientes, de colaboradores ou de terceiros, possuem caráter confidencial e sigiloso, motivo pelo qual comprometo-me a manuseá-las de maneira segura e somente no exercício de minhas atividades, evitando sua perda, furto, cópia, utilização indevida ou divulgação não autorizada;

3. O Cartório está autorizado a consultar e analisar informações registradas em qualquer meio localizado em suas instalações e que tenham sido geradas ou recebidas utilizando seus recursos, inclusive correspondências recebidas em nome ou endereço da organização;

4. Não devo adquirir, reproduzir, utilizar ou distribuir cópias não autorizadas ou legalmente adquiridas de softwares ou programas produtos, mesmo aqueles desenvolvidos internamente pelas áreas técnicas do Cartório;

5. Devo zelar pela segurança, uso correto e manutenção adequada dos equipamentos existentes no Cartório. Adicionalmente, comprometo-me a fazer uso adequado dos canais de comunicação corporativos estando estritamente aderente aos interesses da organização.

6. As informações por mim geradas ou recebidas, em formato impresso ou eletrônico, durante minha jornada de trabalho deverão tratar apenas de assuntos profissionais e ligados exclusivamente ao exercício de minha função; e

7. Descumprindo os compromissos por mim assumidos nesta declaração estarei sujeito às penalidades aplicáveis, como medidas administrativas/disciplinares internas e/ou ações penais/cíveis previstas em lei.

**(Cidade e Data)**

**(Assinatura do Colaborador)**