SEGUNDO OFÍCIO EXTRAJUDICIAL
COMARCA DE NOVA XAVANTINA
ESTADO DE MATO GROSSO

POLÍTCA DE SEGURANÇA DA INFORMAÇÃO DO SEGUNDO OFÍCIO EXTRAJUDICIAL DA COMARCA DE NOVA XAVANTINA-MT

Atualização em 2026.

De acordo com a ISO 270001, que é a norma definidora e reguladora das diretrizes gerais de segurança da informação nas empresas, O Segundo Ofício Extrajudicial da Comarca atualiza as medidas e controles a fim de evitar a perda, vazamento ou ataques contra dados corporativos (principalmente os confidenciais e sensíveis). Esses controles envolvem desde diretrizes gerais de segurança para cumprimento de normas e a realização de procedimentos operacionais de rotina, cujas diretrizes estão documentadas no sistema de Políticas de Segurança da Informação (PSI) da serventia.

A aplicação da **Política de Segurança da Informação** tem por fundamento o planejamento na busca do aumento da integridade, confidencialidade e disponibilidade da informação**,** determinando o caminho que o Segundo Ofício Extrajudicial da Comarca de Nova Xavantina deve seguir com relação à segurança, em todos os aspectos, podendo conter diretrizes para os processos de tratamento de dados, estado em consonância com o que está disciplinado no Manual de Lei Geral de Proteção de Dados e no Manual de Qualidade, Regulamento de Conduta e Política de Privacidade de Dados da própria serventia.

Nesses termos, através da estrutura da PSI do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT, pontos cruciais são estabelecidos:

- Qual o objetivo da política de segurança da informação;
- Quem são as partes interessadas
- O sistema geral de segurança da informação, portanto, a cultura da serventia;
- Diretrizes gerais fornecidas pela PSI;
- Sanções e punições inerentes ao descumprimento das políticas;
- Como lidar com casos omissos;
- Controle de atualização e revisão;

A PSI da serventia extrajudicial é elaborada seguindo três pilares:

- integridade: As informações devem se manter íntegras, confiáveis e condizentes com a realidade, inalteradas, garantindo que as informações não sejam eliminadas ou alteradas sem permissão.
- confidencialidade: As diretrizes documentadas na PSI da serventia devem garantir que os dados coletados, tratados e armazenados, bem como suas fontes e demais sistemas da organização são acessíveis apenas a pessoas específicas a fim de evitar a quebra de confidencialidade das informações, conforme a L. 13.709/2018, NR1 – Disposições Gerais e Gerenciamento de Riscos Ocupacionais e Prov. 213/2026 do CNJ;
- disponibilidade: A serventia, na pessoa de seu delegatário, deve garantir que o acesso aos dados estará disponível a quem é de direito sempre que necessário. Para tanto, a manutenção da área de TI e atos de notas e registro alinhados, bem como os impactos da PSI nas operações.

Etapas seguidas na Política de Segurança da Informação do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT.

1 Diagnóstico de ambiente e contexto organizacional

Todas as medidas que impactam o trabalho de diferentes setores da serventia devem ser levantadas a fim de que se tenha uma visualização ampla sobre todos os processos e tarefas que devem ser cobertos na PSI, a fim de garantir a segurança da informação na organização.

Quanto na parte da TI, deve-se levantar todos os ativos de informação, participar do mapeamento de processos dos atos de Notas e Registro e identificar as limitações de recursos que impactam no cumprimento de uma Política de Segurança da Informação, formulando o mapa do ambiente, contendo elementos como:

- Definição e proposta da PSI para atingir os objetivos da organização;
- Quem são as partes interessadas que serão direta ou indiretamente impactadas pela PSI;
- Quais as regras de negócios que são praticadas pela organização;
- O alinhamento da PSI com leis, normas, regulamentações externas, boas práticas e cultura da empresa;
- Dimensão que a PSI abrange, bem como suas exceções.

2 Levantamento de metas

Devem ser avaliadas pelas equipes de TI e segurança a fim de definir um conjunto de metas alcançáveis e que fazem sentido para a visão, missão e valores da organização, conforme exposto no Manual de Qualidade, Regulamento de Conduta e Política de Privacidade de Dados do Segundo Ofício Extrajudicial.

3 Classificação da confidencialidade das informações

Classificada a confidencialidade das informações, é possível entender se determinado colaborador está tendo acesso a dados críticos e identificar vulnerabilidades.

4 Elaboração das normas de utilização e acesso à informação

As informações coletadas durante o diagnóstico de ambiente devem ser avaliadas sob a ótica da confidencialidade das informações e das metas de negócio. Depois, devem ser definidos os seguintes critérios:

- Quem tem acesso às informações e quais os níveis de permissão?
- Como devem ser utilizadas as aplicações e ativos de informação da empresa?
- Quais são os requisitos mínimos que todos os colaboradores devem seguir para manter as informações confidenciais, íntegras e disponíveis?
- Como utilizar recursos tecnológicos em geral?
- O que deve ser feito em caso de perda ou vazamento de dados, bem como ataques à infraestrutura? Qual é o plano de contingência?

Do lado da TI, é necessário considerar camadas diversas para manter os dados protegidos. Seguir rigorosamente a implementação das boas práticas requisitadas pelos fabricantes dos softwares e aplicações utilizadas pela empresa é um passo crucial. Outra questão é manter boas práticas, por exemplo não expor à internet portas e protocolos com acesso de administrador aos servidores, como é o caso de WTS e SSH. Também é necessário garantir a aplicação de políticas e regras de firewall, bem como manter atualizados seus firmware e mecanismos de antivírus.

5. Implementação das Políticas de Segurança da Informação

Na fase de implementação é essencial que a sua empresa reserve um tempo para aplicar treinamentos, realizar palestras e criar campanhas de conscientização.

Outro ponto importante é realizar avaliações periódicas para manter os critérios das políticas bem fixados para todos, bem como avaliar se as pessoas compreenderam seu papel para a segurança das informações corporativas e se as normas

Dessa forma, o presente Manual de Política de Segurança da Informação visa auxiliar na Elaboração de uma Política de Segurança da Informação, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a serventia extrajudicial, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Segurança da Informação visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação,

Essa Política de Segurança objetiva estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT

6 Escopo

Instituir a Política de Segurança da Informação (PSI), no âmbito do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas. Esta Política se aplica a todos os ativos de informação do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, contratados, parceiros e terceiros que acessam ou processam as informações da serventia. Esta política se aplica em toda instalação física administrada ou utilizada pelo Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT.

7 Termos e definições

Para efeito desse Manual, são aplicáveis as definições previstas na NBR ISO 9001:2008, na ISO 15.906:2010, NR1:2026 em Sistemas de Gestão, em vocabulário.

- ABNT – Associação Brasileira de Normas Técnicas.
- ANONIMIZAÇÃO – utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- ANOREG/BR – Associação dos Notários e Registradores do Brasil.
- BANCO DE DADOS – conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- CPD – Centro de Processamento de Dados.
- CLIENTE – Qualquer entidade, pessoa, órgão ou outro processo que recebe, é usuário/consumidor ou se beneficia dos resultados (produto, serviço ou informação) do processo em questão.
- CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados.
- CONTROLADOR – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- CONSENTIMENTO – manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- DADO PESSOAL – informação relacionada a pessoa natural identificada ou identificável.
- 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.
- DADO ANONIMIZADO: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados
- ENCARREGADO – pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- EMPOWERMENT – Aumento da responsabilidade e autonomia do colaborador quanto à interpretação e execução dos seus procedimentos.
- FORNECEDOR – Entidade, pessoa ou setor que fornece insumos (produto, serviço ou informação) ao processo em questão. Também os fornecedores podem ser externos ou internos.
- HUMANWARE – é um modelo de gerenciamento do fator humano, desenhado para oferecer ferramentas de prevenção, diagnóstico e manejo de

conflitos ao longo do ciclo de vida de um projeto. Trata-se da valorização do ser humano através do desenvolvimento e crescimento pessoal.

- INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Não Conformidade – algo que não está conforme o planejado ou esperado, quando há um erro de processo ou defeito no produto.
- NBR – Norma Brasileira.
- NC – Não Conformidade".
- OPERADOR – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- POPs – Procedimentos Operacionais Padrões.
- PDI – Plano de Desenvolvimento Pessoal.
- PPRA – Programa de Prevenção de Riscos Ambientais.
- PQTA – Prêmio de Qualidade Total ANOREG;
- PROCESSO – Conjunto de atividades pré-determinadas feitas para gerar produtos/serviços que atendam às necessidades dos clientes/usuários. Para isso usa insumos e fornecedores.
- PRODUTO – Parte que cabe a alguém fazer de um serviço ou da confecção de um bem, o qual após o seu término terá continuação com a próxima pessoa no processo de trabalho. Exceto reconhecimento de firma, os atos notariais e de registro são produtos.
- QUALIDADE TOTAL – é uma técnica de administração multidisciplinar formada por um conjunto de Programas, Ferramentas e Métodos, aplicados no controle do processo de produção das empresas, para obter bens e serviços pelo menor custo e melhor qualidade, objetivando atender as exigências e a satisfação dos clientes.
- RAC - Reunião de Avaliação Crítica.
- RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- RINAC: Registro Interno de Não Conformidades.
- SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
- SGQ – Sistema de Gestão de Qualidade.

- TITULAR: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- TRABALHADOR/COLABORADOR/PREPOSTO - pessoa física inserida em uma relação de trabalho, inclusive de natureza administrativa, como os empregados e outros sem vínculo de emprego
- TURNOVER – Entrada e saída de colaborador.
- USO COMPARTILHADO DE DADOS: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

7 **Diretrizes e regras aplicáveis na segurança da informação no Segundo Ofício Extrajudicial da Comarca de Nova Xavantina-MT**

Art. 1º. Fica instituída a Política de Segurança da Informação do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se ao Segundo Ofício Extrajudicial da Comarca de Nova Xavantina, e deverá ser observada por todos os usuários de informação, seja colaborador ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste.

CAPÍTULO

I - Disposições Gerais

Art. 3º. São objetivos da Política de Segurança da Informação: estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos; estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações; estabelecer competências e responsabilidades quanto à segurança da informação; nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação; promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina.

CAPÍTULO II - Dos Princípios e Diretrizes

Art. 4º. As ações de segurança da informação do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina são norteadas pelos princípios constitucionais e administrativos, bem como pelos seguintes princípios: disponibilidade, integridade, confidencialidade e autenticidade das informações; continuidade dos processos e serviços essenciais para o funcionamento do Segundo Ofício; economicidade da proteção dos ativos de informação; respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade; observância da publicidade como preceito geral e do sigilo como exceção; responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação; alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do Segundo Ofício, assim como demais normas específicas de segurança da informação; conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 5º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do Segundo Ofício e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 6º. As normas, procedimentos, manuais e metodologias de segurança da informação do Segundo Ofício Extrajudicial devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 7º. As ações de segurança da informação devem: considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da serventia; ser tratadas de forma integrada; ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; visar à prevenção da ocorrência de incidentes.

Art. 8º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao serviço extrajudicial.

Art. 9. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no Segundo Ofício Extrajudicial da Comarca de Nova Xavantina compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional da serventia, são passíveis de monitoramento e auditoria, respeitados os limites legais.

Art. 10. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação da serventia a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da serventia.

Art. 11. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da serventia, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 12. Todos os contratos de prestação de serviços firmados pela serventia conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como se suas normas decorrentes.

CAPÍTULO III - Da Gestão de Segurança da Informação

Art. 13. A estrutura de Gestão de Segurança da Informação é composta por: Administração; Comitê de Segurança da Informação; Modelo de Política de Segurança da Informação (PSI); Gestor de Segurança da Informação, além de outros possíveis, como, Gestor de Tecnologia da Informação e Comunicação; Encarregado pelo Tratamento de Dados Pessoais; Responsável pela Unidade de Controle Interno; Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e Usuários de Informação.

Art. 14. Compete à Administração:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da serventia, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados. Compõe a Administração: O titular do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina.

Art. 15. Compete ao Comitê de Segurança da Informação:

I. formalizar e aprovar a Política de Segurança da Informação da serventia, bem como suas alterações e atualizações. assessorar na implementação das ações de segurança da informação; constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação; participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação; propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação; deliberar sobre normas internas de segurança da informação; avaliar as ações propostas pelo gestor de segurança da informação.

Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação será definido em ata, de acordo com a legislação vigente. Compõem o Comitê de Segurança da Informação: O titular da serventia, o primeiro substituto, um técnico em informática e a empresa MEDLABOR.

Art. 16. Compete ao Gestor de Segurança da Informação:

I. coordenar o Comitê de Segurança da Informação;
II. coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;
III. assessorar a Administração na implementação da Política de Segurança da Informação;
IV. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
V. promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os colaboradores, usuários e prestadores de serviços que trabalham no serviço extrajudicial;
VI. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação; propor recursos necessários às ações de segurança da informação;
VII. acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

VIII. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

IX. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

Parágrafo único. O Gestor de Segurança da Informação do Segundo Ofício Extrajudicial será designado em ata, de acordo com a legislação vigente. Integra a Gestão de Segurança o titular do serviço extrajudicial e a Empresa Prosix e Empresa MEDLABOR.

Art. 17. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução. Compõe a Gestão de Tecnologia da Informação e Comunicação o titular da serventia, o primeiro substituto, a Empresa Prosix, a Empresa MEDLABOR.

Art. 18. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis, em consonância com o Manual de Qualidade, Regulamento de Conduta e Política de Privacidade de Dados e Manual da Lei Geral de Proteção de Dados do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina. A serventia tem como Encarregados o primeiro substituto e um responsável em tecnologia da informática.

Art. 19. Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na serventia; monitorar as redes computacionais; detectar e analisar ataques e intrusões; tratar incidentes de segurança da informação; identificar vulnerabilidades e artefatos maliciosos; recuperar sistemas de informação; promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em contrato com empresa terceirizada.

Art. 20. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do Segundo Ofício Extrajudicial da Comarca de Nova Xavantina.

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 21. A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 22. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

- tratamento da informação; segurança física e do ambiente; gestão de incidentes em segurança da informação;
- gestão de ativos; gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
- controles de acesso; gestão de riscos; gestão de continuidade; auditoria e conformidade.

§ 1º O Comitê de Segurança da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 23. As políticas, normas, procedimentos, orientações ou manuais de que trata o §2º do art. 16 devem abordar, no mínimo, aspectos relacionados:

I. a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;
II. a classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III. a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
IV. ao uso aceitável da informação e a utilização de mídias de armazenamento;
V. a entrada e saída de ativos de informação das instalações da organização; aos perímetros de segurança da organização;
VI. aos controles de acesso baseados no princípio do menor privilégio;
VII. as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente; aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;
VIII. ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;
IX. a Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização;
X. a manutenção de inventario atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança;
XI. uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências;
XII. o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade;
XIII. a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;
XIV. a utilização adequada dos recursos operacionais e de comunicações fornecidos pela serventia, a serem utilizados para fins profissionais, relacionados às atividades da serventia, em conformidade com os princípios éticos e profissionais da empresa terceirizada, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação do Segundo Ofício Extrajudicial aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;
XV. o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;
XVI. o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;
XVII. as políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a

conformidade com as leis e regulamentos aplicáveis, atualmente Empresas Mundell e Prosix;

XVIII. as políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação do serviço extrajudicial;

XIX. as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente da serventia, dos seus ativos de informação e das ameaças à segurança da informação;

XX. a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento;

XXI. o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos; as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que o serviço extrajudicial possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XXII. as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças; as políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

CAPÍTULO IV – EMPREGO DE TECNOLOGIA DA INFORMAÇÃO – SEGURANÇA, CONTINUIDE, INTEGRIDADE E DISPONIBILIDADE DE DADOS

Art. 24. A Serventia cumpre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro, p. ex., política de mecanismos preventivos de controle físico e lógico envolvendo um plano de continuidade contra ocorrências nocivas ao regular funcionamento do serviço de notas e de registro (CNJ, Prov. 213/2026):

Art. 24-A. Governança, estruturação organizacional e conformidade legal

ETAPA 1

Escopo da etapa: instituir a base normativa, organizacional e documental que viabiliza a conformidade integral com o Provimento 213/2026 do CNJ, assegurando responsabilidade definida, alinhamento à LGPD, controle formal de acessos e prevenção imediata de vulnerabilidades críticas. Condições objetivas de conformidade: ao final desta etapa, o Segundo Ofício Extrajudicial da comarca de Nova Xavantina deverá possuir governança formal instituída, responsabilidades claramente atribuídas, política interna vigente e publicizada, controles mínimos de autenticação implementados, inventário de ativos concluído e base documental apta a demonstrar conformidade inicial em eventual fiscalização correicional.

a) designar formalmente:

I – responsável técnico interno pela implementação;

II – responsável pela serventia como controlador de dados pessoais;

III – encarregado/DPO, quando aplicável.

b) elaborar, aprovar e divulgar internamente a Política de Segurança da Informação, contemplando integralmente os elementos mínimos do Anexo III do Prov. 213/2026 do CNJ, e estabelecendo (planejando), de forma expressa e estruturada, as diretrizes, objetivos estratégicos, cronogramas, responsabilidades e demais parâmetros que fundamentarão a elaboração, na Etapa 2, do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD).

Nesta Etapa 1, exige-se a incorporação dessas diretrizes à Política interna, com definição preliminar de escopo, governança e critérios de continuidade. A formalização técnica completa, operacional e documentada do PCN e do PRD, com definição detalhada de riscos, medidas de mitigação, RTO e RPO, ocorrerá obrigatoriamente na Etapa 2, vedada tanto sua exigência integral nesta Etapa 1 quanto sua postergação para etapa posterior à segunda;

c) implementar autenticação individualizada e autenticação multifator obrigatória para acessos administrativos, vedadas credenciais compartilhadas;

d) instituir registro das operações de tratamento de dados pessoais, nos termos do art. 7º, §1º.

e) incidentes classificados como críticos deverão ser comunicados à Corregedoria competente nos prazos e condições definidos no Anexo II, sem prejuízo das comunicações exigidas pela legislação específica;

f) sem prejuízo do prazo máximo previsto no item anterior, constitui meta de governança e padrão de diligência reforçada que a comunicação à Corregedoria competente ocorra, sempre que possível, em até 24 (vinte e quatro) horas da ciência do incidente, especialmente quando houver risco relevante de indisponibilidade prolongada, comprometimento de dados pessoais ou potencial impacto sistêmico;

g) elaborar inventário completo de ativos tecnológicos, integrações, bancos de dados, certificados digitais, softwares, histórico de atualizações e contratos;

h) regularizar licenciamento de softwares e revisar todos os contratos com terceiros que envolvam tratamento, armazenamento ou processamento de dados da serventia, assegurando cláusulas expressas e exequíveis de:

(i) confidencialidade;

(ii) reversibilidade;

(iii) portabilidade integral do acervo em formato interoperável e não proprietário;

(iv) disponibilização de documentação técnica necessária à migração;

(v) cooperação em caso de transição de fornecedor;

(vi) gestão de incidentes; e

(vii) conformidade integral com a Lei nº 13.709/2018;

h) produzir declaração de conclusão da Etapa 1, a ser necessariamente pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registro da conclusão da Etapa 1 no Sistema Justiça Aberta.

Art. 24-B. Infraestrutura e continuidade operacional

ETAPA II

Escopo da etapa II: estruturar a base material que sustenta os sistemas informatizados, garantindo disponibilidade mínima, estabilidade elétrica, segurança física e planejamento formal de continuidade. Condições objetivas de conformidade: ao término da etapa, a serventia extrajudicial deverá dispor de infraestrutura física adequada, conectividade compatível com sua classe, planos formais de continuidade (PCN e PRD) com RTO e RPO definidos, e capacidade mínima de manter ou restabelecer as operações dentro dos parâmetros normativos.

a) implementar infraestrutura energética adequada (fonte estável, aterramento técnico e SAI/UPS com autonomia mínima de 30 minutos);

b) estabelecer plano de contingência energética compatível com a classe;

c) adequar ambiente físico com controle de acesso restrito e proteção contra incêndio, inundações e variações térmicas.

d) implementar conectividade compatível com a classe, com roteador, switch e, quando necessário, múltiplos links;

e) formalizar o Plano de Continuidade de Negócios (PCN) e o Plano de Recuperação de Desastres (PRD), em documentos distintos ou integrados, desde que contenham, cumulativamente:

I – identificação e avaliação estruturada de riscos;

II – definição objetiva das medidas de mitigação;

III – estabelecimento expresso de RTO e RPO compatíveis com a classe da serventia; e

IV – previsão de medidas de curto prazo (até 30 dias) e de médio prazo (até 90 dias) para resposta a incidentes e restauração da normalidade operacional, sendo vedada a declaração de conclusão da etapa sem a presença de todos esses elementos.

f) garantir disponibilidade de equipamentos adequados e suporte técnico contínuo

g) implementar proteção básica de *endpoint* (antivírus, antimalware ou solução tecnicamente equivalente) em todas as estações e servidores utilizados pela serventia, como condição mínima de integridade operacional da infraestrutura

h) formalizar documento técnico simplificado da arquitetura tecnológica adotada, contendo, no mínimo:

I – topologia básica de rede;

II – indicação dos ambientes utilizados (local, nuvem, híbrido, SaaS ou compartilhado);
III – fluxos de dados críticos;

IV – localização física ou lógica dos *backups;*

V – integrações externas relevantes; e

VI – mecanismos de alta disponibilidade ou redundância.

i) produzir declaração de conclusão da Etapa 2, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

Art. 24-C. Proteção do acervo digital e resiliência tecnológica

ETAPA III

Escopo da etapa: assegurar integridade, confidencialidade e recuperabilidade do acervo eletrônico, prevenindo perda de dados, interceptação indevida e comprometimento sistêmico. Condições objetivas de conformidade: ao final da etapa, todos os dados críticos deverão estar protegidos por criptografia por criptografia adequada, com rotinas automatizadas de *backup* proporcional à classe, armazenamento *off-site,* monitoramento ativo e defesas perimetrais implementadas.

Disposição geral – A implementação das medidas previstas nesta etapa pressupõe o cumprimento integral e comprovado da Etapa 2, não podendo ser declarada concluída enquanto inexistentes ou incompletos os requisitos estruturais de infraestrutura e

continuidade operacional anteriormente estabelecidos. Esta etapa consolida modelo de segurança em camadas (defesa em profundidade), integrando controles de identidade, rede, aplicação e armazenamento. a) implementar criptografia para dados em trânsito e em repouso, inclusive *backups*, com gestão formal de chaves criptográficas que contemple, no mínimo:

I – inventário atualizado de chaves e certificados;

II – segregação de custódia;

III – controle formal de acesso;

IV – política documentada de rotação e renovação periódica;

V – registro das operações de geração, renovação e revogação; e

VI – revisão periódica dos padrões criptográficos adotados.

a) implantar rotinas automatizadas de backup completo e incremental, observando, cumulativamente:

a.I) realização de cópias completas em periodicidade compatível com a classe da serventia, observados os seguintes parâmetros mínimos:

* Classe 3: intervalo não superior a 24 (vinte e quatro) horas. Classe em que se enquadra o Segundo Ofício Extrajudicial da Comarca de Nova Xavantina;

a.II) execução de cópias incrementais compatíveis com o RPO definido para a classe da serventia;

a.III) armazenamento dos dados de *backup* em, no mínimo, dois ambientes tecnicamente independentes, assegurada redundância geográfica ou lógica equivalente, admitidas as seguintes arquiteturas, isoladas ou combinadas:

* ambiente de nuvem com redundância geográfica automática e mecanismos de imutabilidade de dados (WORM, versionamento bloqueado ou tecnologia equivalente);

* mídia eletrônica mantida em local fisicamente distinto das instalações principais *(off-site)*;

* solução híbrida que combine armazenamento local redundante com replicação externa;

* garantia de que pelo menos um dos ambientes de backup esteja protegido contra criptografia maliciosa, exclusão indevida ou comprometimento sistêmico simultâneo, por

meio de mecanismos de isolamento lógico, bloqueio de retenção, controle de acesso reforçado ou tecnologia equivalente.

b) a exigência de múltiplos ambientes tecnicamente independentes poderá ser cumprida exclusivamente por arquitetura em nuvem, desde que demonstrada, por meio de documentação técnica formal, a existência cumulativa de:

I – redundância geográfica automática em regiões distintas;

II – política de retenção imutável com bloqueio contra exclusão administrativa;

III – segregação lógica de acesso;

IV – registro auditável de operações; e

V – viabilidade comprovada de restauração integral do acervo. A escolha da arquitetura de *backup* deverá observar a proporcionalidade regulatória conforme a classe 3 da serventia e as condições socioeconômicas e tecnológicas regionais, vedada solução que implique ponto único de falha ou dependência estrutural não mitigada de fornecedor exclusivo.

c) monitorar rotinas de *backup* com alertas automáticos e registro formal de falhas.

d) implantar fi*rewall statefu*l com IPS/IDS e segmentação lógica de rede.

e) implementar solução avançada de proteção de *endpoint*, quando compatível com a classe da serventia, incluindo monitoramento ativo, detecção de comportamento anômalo ou recursos equivalentes de resposta a incidentes.

f) utilizar SGBD com integridade transacional e logs ativos. -*

g) implementar mecanismos de tolerância a falhas ou alta disponibilidade compatíveis com a classe.

h) implementar trilhas de auditoria técnicas imutáveis, com sincronização de tempo por fonte confiável, identificação inequívoca do usuário, registro de data e hora e mecanismo de verificação de integridade, assegurando sua integração obrigatória às rotinas de *backup* e recuperação, com preservação íntegra e rastreável, observados os prazos mínimos de retenção.

i) produzir declaração de conclusão da Etapa 3, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

Art. 24-D. Monitoramento, auditoria e validação de controles

ETAPA 4

Escopo da etapa: consolidar a rastreabilidade, validar empiricamente os controles implementados e instituir modelo preventivo de gestão de riscos. Condições objetivas de conformidade: ao final desta etapa, a serventia deverá possuir trilhas de auditoria íntegras, monitoramento contínuo, gestão formal de vulnerabilidades, testes documentados de restauração e simulações de desastre validadas.

a) emitir relatório de conformidade de auditoria, atestando a aderência integral das trilhas de auditoria aos requisitos técnicos previstos, mediante procedimento documentado de verificação que comprove, cumulativamente, a imutabilidade, a identificação inequívoca do usuário, a sincronização temporal por fonte confiável, retenção mínima, e a efetiva integração às rotinas d*e backup* e recuperação.

b) o relatório de conformidade deve ser entendido como validação de requisitos estruturais das trilhas de auditoria. Deverá atestar não apenas se o dado "volta", mas se o sistema efetivamente registra quem fez o que, quando fez, se o tempo está sincronizado e se estes registros são realmente imutáveis.

c) instituir rotina documentada de atualização periódica de sistemas e aplicações. d) implementar gestão formal de vulnerabilidades, com:

I – tratamento de vulnerabilidades classificadas como críticas nos prazos e condições definidos no CNJ, Prov. 213/2026, com registro formal das providências adotadas no dossiê técnico;

II – adoção de medidas imediatas de contenção e correção emergencial, preferencialmente em até 72 (setenta e duas) horas, quando houver exploração ativa, risco iminente ou comprometimento relevante já identificado;

III – registro formal, auditável e cronologicamente organizado das providências adotadas, com indicação de responsável e data de conclusão.

e) realizar simulação anual de desastre para validação do PCN e PRD.

f) realizar testes documentados de restauração de backups, conforme periodicidade da classe.

g) realizar avaliações técnicas periódicas de segurança.

h) para as serventias enquadradas na Classe 3, realizar teste de intrusão (pentest) ou metodologia técnica equivalente, observado o disposto no Anexo II, item 6, inclusive quanto às hipóteses de validação coletiva, dispensa condicionada e periodicidade mínima.

i) documentar análise de causa raiz e lições aprendidas para todos os incidentes.

j) produzir declaração de conclusão da Etapa 4, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo a pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

Art. 24-E. Interoperabilidade, consolidação e governança evolutiva

ETAPA 5

Escopo da etapa: integrar o Segundo Ofício Extrajudicial da comarca de Nova Xavantina ao ecossistema de fiscalização, consolidar as evidências documentais produzidas nas etapas anteriores e institucionalizar processo permanente e contínuo de revisão, aprimoramento e evolução tecnológica, vedada interpretação que restrinja as obrigações aqui previstas a momento único ou conclusivo. Condições objetivas de conformidade: ao final desta etapa, o Segundo Ofício deverá estar plenamente integrada às plataformas de fiscalização, com interoperabilidade técnica assegurada, política revisada periodicamente, capacitação contínua implementada e declaração formal de conformidade realizada.

a) adequar sistemas para interoperabilidade com plataformas eletrônicas de fiscalização.

b) adotar padrões abertos e neutralidade tecnológica, prevenindo dependência exclusiva de fornecedor.

c) instituir capacitação periódica com registro formal das ações realizadas.

d) revisar formalmente a Política de Segurança e padrões criptográficos sempre que houver alteração normativa relevante ou evolução tecnológica.

e) manter registros auditáveis por, no mínimo, 5 anos.

f) manter plano formal de reversibilidade e portabilidade de dados, acompanhado de simulação documentada de extração integral do acervo digital em formato interoperável e não proprietário, cuja realização deverá preceder a declaração de conclusão da etapa 5, sendo vedada sua homologação sem evidência técnica de viabilidade concreta de transferência organizada ao sucessor.

I – no mínimo, a cada 24 (vinte e quatro) meses, para as serventias enquadradas na Classe 3;

II – imediatamente, sempre que houver alteração relevante de fornecedor, arquitetura tecnológica ou modelo de governança. Dever-se-á manter registro auditável do procedimento.

g) a simulação documentada de extração integral poderá ser realizada:

I – em ambiente de contingência, réplica, laboratório isolado ou cópia técnica representativa do acervo;

II – por meio de exportação estrutural completa acompanhada de validação técnica de consistência e integridade, admitida verificação por amostragem estatisticamente representativa dos atos eletrônicos;

III – de forma escalonada ou segmentada por módulos ou bases, desde que demonstrada, por evidência técnica formal, a viabilidade concreta de reconstrução integral do acervo.

Quando a serventia demonstrar, por meio de justificativa técnica formal e evidências documentadas, que a realização da simulação integral bienal implica impacto operacional desproporcional em razão do volume do acervo digital, da arquitetura tecnológica adotada ou da limitação estrutural de conectividade, admitir-se-á a substituição da repetição integral por validação técnica estrutural de portabilidade, desde que:

I – seja comprovada a viabilidade concreta de extração integral do acervo por meio de testes segmentados, exportações estruturais completas acompanhadas de verificação de integridade e reconstrução parcial representativa; e

II – a justificativa técnica e as evidências sejam incluídas no dossiê técnico da etapa, sujeitas à fiscalização correicional.

h) produzir declaração de conclusão da Etapa 5, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão da Etapa 5 no Sistema Justiça Aberta.

Art. 25-F os padrões mínimos de tecnologia da informação e comunicação para garantir a segurança, a integridade, a disponibilidade, a autenticidade e a rastreabilidade, assegurando a continuidade das atividades dos serviços notariais e de registro do Brasil

- uniformização dos critérios para a manutenção, guarda e conservação de livros, documentos, arquivos eletrônicos e mídias digitais de segurança que integram o acervo das serventias extrajudiciais, de modo a assegurar padronização procedimental, integridade informacional e eficiência administrativa;
- implementação de padrões modernos de tecnologia da informação e de planos de continuidade de negócios deve observar diretriz de progressividade e proporcionalidade regulatória (CNJ, Prov. 213/2026, art. 6º, IV);
- lavratura de dossiê técnico, organizado, íntegro e verificável de evidências documentais, técnicas e operacionais destinadas a demonstrar o cumprimento de etapa ou requisito específico, apto à fiscalização pela Corregedoria—Geral da Justiça do Estado do Mato Grosso (CNJ, Prov. 213/2025, art. 2º, VI);
- Plano de Continuidade de Negócios (PCN) estruturado de procedimentos destinados a assegurar a continuidade da prestação do serviço em situações de indisponibilidade (CNJ, Prov. 213/2026, art. 2º, X);
- Plano de Recuperação de Desastres (PRD) com as medidas técnicas e operacionais voltadas à restauração de sistemas e dados após incidente grave (CNJ, Prov. 213/2026, art. 2º, XI);
- O delegatário, responsável pelo tratamento de dados pessoais no âmbito da serventia extrajudicial, desde responsável pelo tratamento de dados pessoais no âmbito da serventia extrajudicial, deverá assegurar conformidade com a Lei nº 13.709/2018, adotando medidas técnicas e organizacionais adequadas à proteção de dados (CNJ, Prov. 213/2026, art. 7º);
- quanto a energia elétrica, devidamente aterrada, inclusive no padrão e link de comunicação de dados de Classe 3: 10 megabits;
- a Serventia conta com local técnico (CPD) isolado dos demais ambientes, assim como implantação de divisórias e acessibilidade por meio de controle de acesso restrito aos colabores da área técnica;
- a Serventia dispõe de local refrigerado, próprio para a exigência dos aparelhos e computadores utilizados para a consecução dos serviços;

- em relação ao *backup* (CNJ, Prov. 213/2026): Os livros e atos eletrônicos são arquivados mediantes cópias de segurança, em intervalos não superiores a 24h, utilizando-se, principalmente, o sistema devidamente aterrado, inclusive no padrão e programa da empresa *Prosix*. São geradas imagens que facilitam a recuperação dos atos praticados nas últimas cópias de segurança, em até pelo menos 30 minutos antes da ocorrência. A serventia utiliza, ainda, cópias de segurança em mídia eletrônica e *backup* em nuvem através da Empresa *Mundell,* da mesa forma, armazenadas em local distinto da serventia;
- em atendimento aos padrões mínimos elencados no anexo do Prov. 213/2026 do CNJ: Os padrões mínimos estabelecidos no anexo, cuja serventia está enquadrada na classe 3, estão sendo implantados, praticamente atingindo 100%, inclusive com o licenciamento de todos os s*oftwares*, p.ex., Windows 10. Portanto, presente o serviço de cópias de segurança da internet, com *backup* em nuvem (Empresas *Prosix* e *Mundell,* responsáveis pelo procedimento) (CNJ, Prov. 213/2026, art. 4º);
- autonomia estrutural, em virtude da serventia deter controle técnico suficiente sobre a continuidade operacional, os mecanismos essenciais de segurança e a extração integral e migrável do acervo, inexistindo dependência estrutural de fornecedor para a continuidade, atualização ou administração essencial da solução (CNJ, Prov. 213/2026, art. 2º, XX);
- a Serventia está aparelhada com *switch* para conexão de equipamentos internos, roteador para controle de coxões externas e internas, *softwares* licenciados, *firewall e prosy* (controle de acesso externo).
- o titular do Segundo Ofício e seus colaboradores, inclusive prepostos e fornecedores, utilizam mecanismos de autenticação individualizados e compatíveis com seus perfis de acesso, com as funções efetivamente exercidas e com o grau de risco associado às atividades desempenhadas (CNJ, Prov. 213/2026, art. 5º);
- o Segundo Ofício Extrajudicial está implantando mecanismos de proteção perimetral aptos a controlar o tráfego de entrada e saída de dados, impedir acessos não autorizados e registrar eventos relevantes de segurança, compatíveis com sua classe e com a criticidade de suas operações;
- manter configuração formalmente documentada, passível de verificação pela Corregedoria competente. Os dados sensíveis, informações pessoais, registros eletrônicos e demais informações armazenadas ou transmitidas no âmbito das serventias deverão ser protegidos por mecanismos de criptografia adequados ao estado da técnica, observadas as boas práticas reconhecidas e os padrões mínimos definidos neste Provimento.

- a Serventia dispõe de colaboradores e pessoas treinadas na operação do sistema e das cópias de segurança, em especial a Empresa *Prosix*, devidamente contratada para assegurar o serviço de manutenção técnica com suporte.
- em relação à transmissão de todo o acervo eletrônico e continuidade da prestação do serviço, e caso de sucessão (CNJ, Prov. 213/2026, art. 6º, III): A serventia está 100% apta para transmitir todo o acervo pertencente, bem como senhas e dados necessários, com total garantia da continuidade da prestação do serviço de forma eficiente e ininterrupta, em caso de sucessão.

CAPÍTULO V - Das Vedações e Disposições Finais

Art. 24. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo Segundo Ofício Extrajudicial da Comarca de Nova Xavantina para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 25. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela serventia

. Art. 26. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 27. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 28. O Segundo Ofício Extrajudicial da Comarca de Nova Xavantina deve promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 29. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais: [inserir lista de canais de denúncia]

Art. 30. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela empresa terceirizada especialista em segurança da informação, periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de

responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 31. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 32. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da serventia, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Elaborado por MARCOS ROBERTO HADDAD CAMOLESI