STM SUPERIOR TRIBUNAL MILITAR
DIDOC/COGES/LEGIS

Publicado no BJM nº 47,
de 1º/12/2023

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

RESOLUÇÃO Nº 340, DE 27 DE NOVEMBRO DE 2023

Institui a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da Justiça Militar da União.

O SUPERIOR TRIBUNAL MILITAR, no uso de suas atribuições legais e regimentais e, tendo em vista a decisão do Plenário na 11ª Sessão Administrativa, realizada em 27 de novembro de 2023, ao apreciar o Expediente Administrativo nº 60/2023, e

CONSIDERANDO que o Código Penal, em seu art. 305, preceitua que é crime punível com a pena de 2 (dois) a 6 (seis) anos de reclusão e multa destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor;

CONSIDERANDO que é dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação, conforme previsto no art. 1º da Lei nº 8.159, de 8 de janeiro de 1991, que "*Dispõe sobre a política nacional de arquivos públicos e privados*";

CONSIDERANDO que a Lei nº 9.605, de 12 de fevereiro de 1998, que "*Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente*", tipifica, em seu art. 62, a destruição de arquivo protegido por lei, ato administrativo ou decisão judicial, como crime contra o patrimônio cultural;

CONSIDERANDO as determinações sobre a geração, a tramitação, o acesso e a guarda de processos judiciais e documentos em meio eletrônico, constantes na Lei nº 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial e altera o Código de Processo Civil;

CONSIDERANDO a Resolução n° 324, de 30 de junho de 2020, do Conselho Nacional de Justiça (CNJ), que "*Institui diretrizes e normas de Gestão de Memória e de Gestão Documental e dispõe sobre o Programa Nacional de Gestão Documental e Memória do Poder Judiciário - Proname*";

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

CONSIDERANDO a Resolução nº 240, de 19 de abril de 2017, que "*Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, na Justiça Militar da União e*

dá outras providências";

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);

CONSIDERANDO a Resolução nº 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que "*Estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais*";

CONSIDERANDO o Decreto nº 8.777, de 11 de maio de 2016, que "*Institui a Política de Dados Abertos do Poder Executivo Federal*"; e

CONSIDERANDO a importância de instituir uma política interna de gestão da informação, do conhecimento e dos dados,

R E S O L V E:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir a Política de Governança Arquivística, da Informação, dos Dados e do Conhecimento, no âmbito da Justiça Militar da União (JMU).

Parágrafo único. A Governança Arquivística, da Informação, dos Dados e do Conhecimento, na Justiça Militar da União, será efetivada pelos seguintes instrumentos:

I - Plano Operacional de Gestão Documental da JMU;

II - Plano Operacional de Gestão e Privacidade de Dados Pessoais;

III - Plano Operacional de Gestão e Difusão de Dados Abertos; e

IV - Plano Operacional de Gestão da Informação e do Conhecimento.

Art. 2º Para os efeitos desta Resolução, consideram-se:

I - cadeia de custódia: manutenção ininterrupta da custódia de dados e documentos, desde o seu produtor até o seu legítimo sucessor, pela qual se assegura que esses dados e documentos são os mesmos desde sua criação e não sofreram nenhum processo de adulteração, portanto, são autênticos, realizada por meio de registros de controles, transferências, análises e disposição de evidências físicas ou eletrônicas, e atestados em metadados padronizados, que asseguram o histórico de alterações e guarda dos dados e documentos;

II - ciclo de vida: as sucessivas fases pelas quais passam os documentos de um arquivo, desde sua produção até sua guarda permanente ou eliminação;

III - tratamento de dados: qualquer atividade pertencente ao ciclo de vida dos dados pessoais;

IV - confidencialidade: propriedade ~~de~~ pela qual se

assegura que a informação não esteja disponível ou não seja revelada à pessoa física, ao sistema, ao órgão ou às entidades não autorizadas ou credenciadas;

V - conhecimento explícito: aquele que pode ser expresso em uma linguagem formal e sistemática, compartilhado em dados, documentos, especificações e manuais e que pode ser processado, transmitido e armazenado com facilidade;

VI - conhecimento tácito: aquele tipo de conhecimento difícil de ser formalizado e transmitido às outras pessoas, relacionado às experiências, à visão de mundo e às práticas de determinado indivíduo;

VII - controlador: pessoa jurídica de direito público, a quem compete definir todas as ações relativas ao tratamento dos dados pessoais, cuja função não poderá ser exercida por pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos;

VIII - encarregado: pessoa física ou jurídica responsável por, dentre outras atribuições, realizar a comunicação entre a Autoridade Nacional de Proteção de Dados, os titulares dos dados e o Controlador, bem como conhecer detalhadamente todo o tratamento efetivado de dados pessoais na instituição;

IX - operador: pessoa física ou jurídica de direito público ou privado que realiza o tratamento em nome do controlador, cuja atividade não poderá recair sobre subordinados, tais como magistrados, servidores públicos ou equipes de trabalho que já atuam diretamente sob o poder diretivo do controlador e o integram, expressando a atuação deste;

X - autoridade nacional de proteção de dados pessoais: órgão vinculado à Presidência da República, ao qual caberá, dentre outras atribuições, fiscalizar a aplicação da LGPD nas entidades do poder público e aplicar sanções em caso de descumprimento de suas determinações;

XI - dado: registro aleatório correspondente à unidade básica da informação bruta; são fatos ou observações que podem ser coletados, registrados e armazenados para posterior análise e processamento, representados em formatos digitais e manipulados por sistemas de computador, podendo ser estruturados ou não estruturados;

XII - dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

XIII - dados abertos: conjunto de dados governamentais produzidos, acumulados, coletados ou custodiados por autoridades públicas, em decorrência de suas atividades, disponibilizados em formato aberto, e que podem ser utilizados, reutilizados e redistribuídos por qualquer pessoa, sem restrições de direito de autor, patente ou outro mecanismo de controle, sujeitos às exigências de citação das fontes;

XIV - *file server* - computador conectado a uma rede que fornece um local para acesso ao disco compartilhado, ou seja, constitui um armazenamento de arquivos de computador, tais como texto, imagem, som, vídeo, que podem ser acessados pelas estações de trabalho, as quais são

capazes de alcançar o computador que compartilha o referido acesso, por meio de uma rede de computadores;

XV - gestão do conhecimento: conjunto de ações e mecanismos consistentes na sistematização das informações e conhecimentos da Justiça Militar da União, englobando várias etapas, desde sua criação até seu armazenamento e disseminação;

XVI - governança arquivística: atividade de gerir e atuar em um conjunto de políticas, programas e projetos de aspectos teóricos-operacionais, com vistas à eficiência e à eficácia, mobilizados pelo profissional da documentação e informação, que atua em um serviço ou uma instituição arquivística;

XVII - informação: dados estruturados, utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XVIII - integridade: qualidade da informação não modificada ou destruída, inclusive quanto à origem, trânsito e destino;

XIX - não repúdio: medida que visa garantir que o autor não negue a autoria do documento ou da informação;

XX - organicidade: qualidade segundo a qual os arquivos espelham a estrutura, funções e atividades da entidade produtora/acumuladora, em suas relações internas e externas;

XXI - segurança da informação: conjunto de medidas e ações necessárias para garantir que a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações de uma organização ou indivíduo sejam preservadas; e

XXII - RDC-Arq: sigla de Repósitório Arquivístico Digital Confiável, que designa um ambiente que oferta preservação e acesso, voltado a documentos de cunho arquivístico em formato digital.

CAPÍTULO II

DA GOVERNANÇA ARQUIVÍSTICA, DA INFORMAÇÃO, DOS DADOS E DO CONHECIMENTO

Seção I

Da Governança Arquivística

Art. 3º A gestão documental, pilar da governança arquivística, constitui o conjunto de procedimentos técnicos e operacionais referentes às atividades de produção, classificação, tramitação, acesso, uso, avaliação e arquivamento, que acontecem nas fases corrente e intermediária, independentemente do suporte em que a informação se encontre registrada, objetivando a manutenção, a eliminação adequada ou o recolhimento dos documentos para a guarda permanente.

Art. 4º Os atributos principais do documento arquivístico institucional são a originalidade, a organicidade, a unicidade, a fidedignidade, a integridade, a autenticidade, a imparcialidade e o não repúdio.

Art. 5º O ciclo de vida dos documentos institucionais é dividido nas seguintes fases:

I - corrente: aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes;

II - intermediário: aqueles que, embora não sendo de uso corrente nas unidades geradoras, por razões de interesse jurisdicional ou administrativo, aguardam sua eliminação ou recolhimento para a guarda permanente;

III - permanente e/ou histórico: aqueles de valor histórico, probatório e informativo, que devem ser definitivamente preservados, conforme estabelecido pela Tabela de Temporalidade e Destinação da Justiça Militar da União - TTD - JMU.

Art. 6º O Ministro-Presidente é a autoridade responsável pela viabilidade da Política de Gestão Documental e pelo apoio integral à sua implantação no âmbito da Justiça Militar da União, alocando recursos humanos, materiais e financeiros.

Art. 7º A gestão documental é operacionalizada por meio de planejamento, organização, controle e coordenação dos recursos humanos, do espaço físico e dos equipamentos, a fim de aperfeiçoar e de simplificar o ciclo documental, tendo como princípios:

I - a manutenção dos documentos em ambiente seguro, garantindo o acesso ininterrupto e os atributos de originalidade, organicidade, unicidade, fidedignidade, integridade, autenticidade, imparcialidade e não repúdio;

II - a adoção de estratégias de preservação dos documentos, desde a sua produção até a destinação final (eliminação ou guarda permanente);

III - a utilização dos instrumentos operacionais da Política de Gestão Documental da Justiça Militar da União;

IV - a racionalização e a padronização das espécies, tipos, classes, assuntos e registros de movimentação de documentos e processos;

V - o uso de critérios obrigatórios de transferência e de recolhimento de documentos às unidades de arquivo, independentemente do tipo de suporte envolvido; e

VI - a utilização do Modelo de Requisitos para Sistemas Informativos de Gestão de Processos e Documentos do Poder Judiciário (MoReq-Jus).

Art. 8º São instrumentos da Política de Gestão Documental da Justiça Militar da União, entre outros:

I - o Plano de Classificação e Tabela de Temporalidade e Destinação da JMU;

II - o sistema informatizado de gestão de processos e documentos administrativos;

III - o sistema informatizado de gestão de processos e documentos judiciais; e

IV - os normativos e manuais aplicáveis à gestão

documental.

Art. 9º Fica criada a Comissão Permanente de Avaliação e Apoio Técnico à Gestão Documental da Justiça Militar da União (CPAD-JMU).

§ 1º A CPAD-JMU será subordinada diretamente ao Ministro-Presidente.

§ 2º Na apuração de possíveis irregularidades ou de indícios de ilícitos cometidos pelas unidades administrativas da Justiça Militar da União, a CPAD-JMU poderá efetuar consulta formal à Assessoria Jurídica do Diretor-Geral (ASJUR) ou, em sendo o caso, à Assessoria Jurídico-Administrativa da Presidência (ASPRE-ADM), acerca dos aspectos jurídicos relativos ao caso analisado.

§ 3º A composição da CPAD-JMU será instituída por Ato Normativo e deverá conter, no mínimo:

I - o titular da DIDOC, que a presidirá;

II - 1 (um) servidor da Seção de Arquivo Corrente e Gestão Documental (SEDOC);

III - 1 (um) servidor da Coordenadoria de Preservação e Difusão da Memória Institucional (CODIM);

IV - 1 (um) servidor da Diretoria de Tecnologia da Informação (DITIN);

V - 1 (um) servidor graduado em curso superior de Arquivologia;

VI - 1 (um) servidor graduado em curso superior de História;

VII - 1 (um) servidor graduado em curso superior de Direito; e

VIII - membro *ad hoc*.

Seção II

Da Governança do Conhecimento

Art. 10. A Gestão do Conhecimento tem por objetivos:

I - desenvolver e incentivar a cultura da criação e disseminação do conhecimento entre os servidores, entre as unidades organizacionais e entre esses e a sociedade;

II - garantir mecanismos formais de retenção e transferência do conhecimento tácito e explícito das atividades-meio e atividades-fim da instituição; e

III - ampliar a eficiência, eficácia e efetividade dos serviços prestados pela Instituição no combate à má gestão de recursos públicos.

Art. 11. As estratégias da Gestão do Conhecimento incluem:

I - identificação, produção, armazenamento, disseminação e aplicação do conhecimento necessário para o desenvolvimento eficiente das atividades-meio e atividades-fim da JMU;

II - formalização de manuais com as rotinas básicas e a garantia de sua constante atualização e progressiva expansão;

III - implementação de recursos tecnológicos a fim de permitir aos servidores a inserção de conteúdo e a consulta às informações, fluxogramas e modelos, de forma intuitiva e dinâmica;

IV - gestão de fontes de informação de bibliotecas e pesquisas legislativas, para fomento e criação de novos conhecimentos;

V - instituição de banco de dados de perfis funcionais, visando melhor aproveitamento das capacidades e aptidões individuais de cada servidor; e

VI - adoção da prática de realização periódica de eventos de capacitação e treinamento, possibilitando o compartilhamento de informações e experiências profissionais.

Art. 12. São instrumentos da Política de Gestão do Conhecimento da Justiça Militar da União, entre outros:

I - acervo bibliográfico, legislativo e jurisprudencial da JMU; e

II - sistemas de informação de difusão e disseminação do conhecimento explícito.

Seção III

Da Governança da Informação e dos Dados Pessoais e Orgânicos Abertos

Art. 13. A gestão da informação incluirá rotinas de processamento, armazenamento, classificação, identificação, organização, segurança e compartilhamento de registros e dados, sejam eles digitais ou físicos.

Art. 14. O tratamento dos dados pessoais e dados orgânicos abertos abrangem aspectos físicos, tecnológicos e humanos e orienta-se pelos princípios de autenticidade, confidencialidade, disponibilidade e integridade, e pelas seguintes disposições:

I - promover ações destinadas a garantir a privacidade e segurança dos dados pessoais e dos dados sensíveis;

II - promover ações de comunicação, conscientização, formação de cultura e direcionamento institucional, com vistas à segurança da informação e dos dados pessoais;

III - orientar ações relacionadas:

a) à proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com legislação específica;

b) ao tratamento das informações com restrições de acesso;

c) à gestão e enfretamento a incidentes de vazamento de dados pessoais;

d) ao estabelecimento dos níveis de maturidade em segurança dos dados pessoais; e

e) ao estabelecimento de processo transparente de dados orgânicos abertos entre o poder público e a sociedade.

IV - promover a publicação de dados contidos em bases de dados sob a forma de dados abertos;

V - aprimorar a cultura da transparência pública;

VI - franquear aos cidadãos o acesso, de forma aberta, aos dados orgânicos produzidos ou acumulados pela JMU, sobre os quais não recaia vedação expressa de acesso; e

VII - facilitar o intercâmbio de dados entre órgãos públicos e a sociedade.

Art. 15. O tratamento de dados pessoais, inclusive nos meios digitais, na Justiça Militar da União, será realizado pelos seguintes agentes:

I - controlador;

II - encarregado; e

III - operador, quando necessário.

§ 1° O controlador, por força da desconcentração administrativa, é o Superior Tribunal Militar, e o exercício da função será atribuído aos Magistrados e Servidores.

§ 2° A função de encarregado será exercida pelo Ministro-Ouvidor.

§ 3° A função de operador será exercida sempre por pessoa distinta do controlador, conforme definição contida no inciso IX do art. 2° desta Resolução.

Art. 16. Fica criado o Comitê Executivo de Privacidade e Dados Orgânicos Abertos – CESDA, subordinado diretamente ao Controlador.

§ 1º As atribuições do CESDA serão instituídas por Ato Normativo.

§ 2º Caberá ao CESDA assessorar os controladores e o encarregado da Justiça Militar da União.

§ 3º A composição do CESDA será instituída por Ato Normativo e deverá conter, no mínimo:

I - 1 (um) servidor da DIDOC, que o presidirá;

II - 1 (um) membro do Comitê Executivo do SEI;

III - 1 (um) servidor da DITIN;

IV - 1 (um) servidor da Corregedoria da Justiça Militar da União (CORJMU); e

V - membro *ad hoc*.

Art. 17. Os órgãos da Justiça Militar da União poderão realizar o tratamento mínimo dos dados pessoais, necessários e imprescindíveis à garantia do interesse público e à execução de suas funções jurisdicional e administrativa.

§ 1º O tratamento dos dados pessoais deverá ser realizado durante todo o ciclo de vida dos documentos.

§ 2º Para a eliminação dos dados pessoais será utilizado o Plano de Classificação e Tabela de Temporalidade da JMU.

Art. 18. Os dados orgânicos abertos, disponibilizados pela Justiça Militar da União, e as informações de transparência ativa são de livre utilização pela sociedade.

§ 1º Fica autorizada a utilização gratuita das bases de dados, cujo detentor de direitos autorais patrimoniais seja a União.

§ 2º Não será permitido nenhum instrumento jurídico que impeça a reutilização e redistribuição, por qualquer membro da sociedade, dos dados abertos da Justiça Militar da União.

§ 3º Serão disponibilizados dados em estado bruto, para serem livremente manipulados, filtrados ou cruzados com outros, inclusive permitindo a construção de novas aplicações e conhecimentos.

Art. 19. A matriz de priorização e limites dos dados orgânicos abertos será regulamentada em norma própria.

CAPÍTULO III

DO ACESSO, DA PRESERVAÇÃO E DA DIFUSÃO DOS DOCUMENTOS E DADOS DA JMU

Seção I

Da Transparência, Do Acesso à Informação, aos Dados e aos Documentos

Art. 20. O direito fundamental de acesso aos dados pessoais, aos dados orgânicos abertos e aos documentos é assegurado nos termos desta Resolução e executado em conformidade com os princípios básicos da Administração Púbica, observando-se as seguintes diretrizes:

I - garantia de acesso à informação e aos dados de forma objetiva;

II - divulgação de informações de interesse público;

III - observância da publicidade como preceito geral e do sigilo como exceção, atendendo aos critérios de respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e às garantias individuais, conforme a legislação pertinente; e

IV - utilização de meios de comunicação viabilizados pela tecnologia da informação.

Parágrafo único. O direito de acesso à informação será franqueado mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.

Art. 21. O acesso e a difusão dos documentos arquivísticos devem cumprir os preceitos legais relativos à preservação do patrimônio histórico e cultural brasileiro.

§ 1º Os procedimentos para o acesso, a divulgação, o manuseio, a reprodução, o transporte, o arquivamento e a guarda de documentos e de processos no âmbito da Justiça Militar da União deverão assegurar, no que couber, a aplicação das normas referentes ao sigilo e ao segredo de justiça.

§ 2º O empréstimo de documentos atenderá aos requisitos de segurança da informação, a fim evitar extravios e danos ao suporte.

§ 3º É vedado o empréstimo ou a reprodução de documentos que apresentem condições de fragilidade que acarretem risco a sua conservação em caso de manuseio.

Art. 22. O Superior Tribunal Militar deverá publicar, em lugar de fácil acesso e visualização em seu portal na internet:

I - as hipóteses que fundamentam a realização do tratamento de dados pessoais;

II - a previsão legal, a finalidade e os procedimentos para tratamento de dados pessoais;

III - a identificação do controlador e do encarregado, com os respectivos contatos de correio eletrônico;

IV - as responsabilidades dos operadores envolvidos no tratamento; e

V - os direitos do titular, com menção expressa ao art. 18 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).

Art. 23. O portal de dados orgânicos abertos da JMU deve garantir os seguintes requisitos técnicos:

I **-** controle de acesso: somente as pessoas autorizadas deverão ter acesso para publicação e modificação dos dados e metadados;

I I **-** integridade: assegurar que os dados não sejam adulterados durante a transferência; e

III **-** autenticidade: assegurar que os dados provêm de uma fonte legítima da Justiça Militar da União.

Seção II

Da Preservação dos Documentos Físicos

Art. 24. A preservação de documentos analógicos é feita pela adoção de técnicas normatizadas e de ações cotidianas de precauções, visando estabelecer critérios para o adequado manuseio, controle ambiental, higienização, iluminação, mobiliários apropriados, conservação preventiva, controle de pragas, acondicionamento, restauro, prevenção contra sinistros, projetos de engenharia, entre outros inerentes ao tema.

§ 1º As ações previstas no *caput* deste artigo constituem medidas consolidadas para otimizar a durabilidade dos suportes, objetivando, sobretudo, a salvaguarda da informação registrada.

§ 2º Com vistas à preservação da documentação e a fim de diminuir o manuseio dos documentos originais, serão desenvolvidas ações para digitalizar, autenticar e descrever o acervo.

§ 3º Os documentos de guarda permanente não poderão ser eliminados, mesmo que digitalizados.

Seção III

Da Preservação de Documentos Digitais

Art. 25. A preservação de documentos digitais estabelecer-se-á por meio de padrões e de procedimentos operacionais necessários ao atendimento dos requisitos de preservação digital.

Parágrafo único. A preservação de documentos digitais engloba todos os documentos arquivísticos nato-digitais ou digitalizados, judiciais ou administrativos, produzidos ou recebidos pela Justiça Militar da União, em decorrência de suas atividades, entre eles:

I - processos digitais, judiciais e administrativos;

II - informações arquivísticas produzidas nos sistemas de negócios do Tribunal;

III - gravações digitais de som e imagem;

IV - fotografias digitais;

V - páginas intranet e internet;

VI - bases de dados digitais;

VII - publicações digitais; e

VIII - mensagens de correio eletrônico, quando se tratar de assunto institucional.

Art. 26. A preservação de documentos digitais da Justiça Militar da União deverá:

I - assegurar as condições adequadas ao pleno acesso aos documentos digitais, pelo prazo institucionalmente estabelecido;

II - assegurar, permanentemente, a autenticidade dos documentos digitais;

III - implantar um repositório arquivístico digital confiável para o gerenciamento da preservação digital; e

IV - preservar o suporte em que os documentos estejam registrados, observando os critérios normativos, nacionais e internacionais, de durabilidade e de compatibilidade com *hardwares*, *softwares* e formatos.

Art. 27. Os documentos serão preservados, preferencialmente, em suas formas, formatos e suportes originais, exceto quando as justificativas e as condições técnicas sobre preservação orientarem o contrário.

Art. 28. A preservação digital tem como princípios:

I - organização e preservação dos documentos digitais e de todos os seus componentes, de modo a garantir a disponibilidade plena desses registros no futuro;

II - integridade e confiabilidade das informações custodiadas, de modo a garantir a segurança dos documentos e evitar a corrupção e a perda de dados;

III - garantia de autenticidade dos documentos;

IV - respeito à propriedade intelectual;

V - observância do sigilo e da restrição de acesso às

informações sensíveis;

VI - transparência ativa;

VII - descrição multinível de documentos digitais avaliados como de guarda permanente; e

VIII - avaliação arquivística de acordo com o Plano de Classificação e Tabela de Temporalidade da JMU.

Art. 29. Os objetivos fundamentais da preservação digital são:

I - implantar e manter Repositório Arquivístico Digital Confiável – RDC-Arq;

II - tornar público o contexto de implantação da preservação digital, bem como os requisitos legais e os normativos que regem o tema, com os quais o Tribunal deverá estar em conformidade;

III - fundamentar a definição dos procedimentos e as opções tecnológicas a serem adotadas no tratamento da informação digital;

IV - divulgar as estratégias adotadas com relação à abordagem de preservação digital, de modo a propiciar o seu aperfeiçoamento contínuo;

V - assegurar as condições adequadas ao pleno acesso a documentos digitais, pelo prazo institucionalmente estabelecido, e respeitado o Plano de Classificação e Tabela de Temporalidade da JMU;

VI - zelar pela cadeia de custódia de modo permanente, com o intuito de garantir a autenticidade dos documentos digitais;

VII - contribuir para a cultura da gestão de risco em segurança da informação;

VIII - promover o intercâmbio de informações e experiências com entidades públicas e privadas, nacionais e internacionais, com vistas à constante atualização e aperfeiçoamento das normas e procedimentos de preservação digital do Tribunal;

IX - fomentar a capacitação na área de preservação digital; e

X - estabelecer atributos e soluções para o armazenamento no *file server.*

Art. 30. Os requisitos de preservação digital adotados e os padrões e procedimentos operacionais necessários à sua implantação serão normatizados pelo Plano de Preservação de Documentos Digitais (PPDD) e amplamente divulgados, sendo oferecida aos interessados a devida orientação técnica.

Art. 31. A produção, o recebimento e a captura de documentos digitais, no âmbito do Tribunal, obedecerão aos seguintes requisitos de preservação digital:

I - classificação arquivística dos documentos em sua origem, de acordo com as normas vigentes referentes à Gestão Documental;

II - registro do conjunto mínimo de metadados descritivos de preservação dos documentos;

III - observância da padronização de formatos de arquivos para documentos de guarda longa ou permanente;

IV - migração de *hardware*, *software*, formato e metadados, com informações técnicas que permitam avaliar a qualidade da migração;

V - observância da cadeia de custódia e da cadeia de preservação digital;

VI - padronização das mídias de gravação e armazenamento; e

VII - capacidade de migração automática de formatos, a fim de superar a obsolescência tecnológica e digital, sem intervenção manual, sem rompimento da cadeia de custódia e sem perda de autenticidade.

CAPÍTULO IV

DO SIGILO DOS DADOS PESSOAIS E DO CONTROLE DE ACESSO

Art. 32. O acesso aos dados pessoais e sensíveis é franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

§ 1º O acesso às informações não públicas produzidas ou custodiadas deverá permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso às informações não públicas por quaisquer colaboradores será condicionado ao aceite de termo de sigilo e responsabilidade.

Art. 33. Todos os usuários que manipulem ou tenham acesso a informações identificadas como sigilosas, sob custódia ou de propriedade da JMU, deverão garantir a confidencialidade e o segredo dessas informações.

Parágrafo único. Sem autorização, é vedada qualquer forma de impressão, transmissão, compartilhamento ou transporte de dados pessoais para fora das instalações da JMU.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 34. Compete aos magistrados, servidores, colaboradores da JMU e usuários de tecnologia da informação e comunicação:

I - adotar os dispositivos legais e normas internas referentes ao sigilo e a outros requisitos de classificação para acesso às informações;

II - zelar pelos dados pessoais sob sua custódia, conforme os critérios definidos em normativos;

III - comunicar, tempestivamente, ao Comitê Executivo de Proteção dos Dados Pessoais situações que comprometam a segurança da

informação sob sua custódia;

IV - comunicar ao Comitê Executivo de Proteção dos Dados Pessoais eventuais limitações ao cumprimento dos critérios definidos para a proteção de dados pessoais;

V – incorporar nos processos de trabalho práticas inerentes à segurança dos dados pessoais;

VI - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de violação à Política de Segurança da Informação; e

VII - implementar controles e monitoramentos de segurança pertinentes, sob a orientação técnica da Diretoria de Tecnologia da Informação (DITIN) e da Diretoria de Documentação e Gestão do Conhecimento (DIDOC).

Art. 35. A DIDOC e a DITIN serão responsáveis pelo planejamento, elaboração e manutenção de sistemas informatizados para a gestão e a preservação de processos e de documentos digitais, administrativos ou judiciais.

Parágrafo único. A DIDOC será responsável pela proposição e atualização de normas e ações para a execução da política de Governança Arquivística, da Informação, dos Dados e do Conhecimento na Justiça Militar da União.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 36. No processo de monitoramento e controle das ações de implantação da Política de Privacidade dos Dados Pessoais e dos Dados Orgânicos Abertos serão observados os indicadores e as principais demandas encaminhadas à JMU, provenientes de reclamações recebidas pela Agência Nacional de Proteção de Dados e pela Ouvidoria da Justiça Militar da União (OUVJMU).

Art. 37. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela JMU devem observar, no que couber, as disposições desta Resolução.

Art. 38. A inobservância dos dispositivos desta Resolução poderá acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 39. Os casos omissos serão resolvidos pelo Ministro-Presidente, ouvida a Diretoria de Documentação e Gestão do Conhecimento.

Art. 40. Ficam revogadas:

I - a Resolução nº 265, de 29 de maio de 2019; e

II - a Resolução nº 298, de 4 de agosto de 2021.

Art. 41. Esta Resolução entra em vigor na data de sua publicação.

Ten Brig Ar **FRANCISCO JOSELI PARENTE CAMELO**

Ministro-Presidente

Documento assinado eletronicamente por **FRANCISCO JOSELI PARENTE CAMELO**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 30/11/2023, às 19:02 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3503922** e o código CRC **4E3E6FA3**.

Setor de Autarquias Sul, Praça dos Tribunais Superiores - Bairro Asa Sul - CEP 70098-900 - Brasília - DF - http://www.stm.jus.br/