PORTARIA PRESIDÊNCIA Nº 339, DE 7 DE OUTUBRO DE 2024.

Dispõe sobre o Uso dos Recursos de Tecnologia da Informação e Comunicação no âmbito do Conselho Nacional de Justiça.

O PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ), no uso das atribuições legais e regimentais, e tendo em vista o contido no processo SEI/CNJ nº 00544/2024,

CONSIDERANDO o disposto na Portaria Presidência n° 47/2017, que institui a Política de Segurança da Informação do Conselho Nacional de Justiça;

CONSIDERANDO o disposto na Instrução Normativa n° 86/2021, que dispõe sobre a governança e a gestão negocial das Soluções de Tecnologia da Informação e serviços digitais do CNJ;

CONSIDERANDO o disposto na Portaria Presidência n° 197/2023, que dispõe sobre a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do Conselho Nacional de Justiça;

CONSIDERANDO que os recursos de Tecnologia da Informação e Comunicação são ativos estratégicos e suportam processos institucionais importantes para os usuários internos e externos do CNJ;

CONSIDERANDO a necessidade de estabelecer diretrizes e procedimentos para o uso adequado e eficiente dos recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito do Conselho Nacional de Justiça;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º O uso dos recursos de Tecnologia da Informação e Comunicação no âmbito do Conselho Nacional de Justiça fica disciplinado por esta Portaria.

§ 1º Compete ao Departamento de Tecnologia da Informação e Comunicação (DTI) a gestão dos recursos computacionais instalados no ambiente tecnológico do CNJ ou gerenciados por ele, em conformidade com os normativos vigentes e as melhores práticas de segurança da informação.

§ 2º As medidas previstas nesta instrução aplicam-se a todos os usuários do ambiente tecnológico do CNJ, acarretando sua responsabilização em função de descumprimento, nos termos previstos em lei e demais regulamentos.

Art. 2º Para efeitos desta Portaria, considera-se:

I – acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de órgão ou entidade, observada eventual restrição que se aplique;

II – ambiente tecnológico: redes, dispositivos, *softwares*, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;

III – banco de dados: coleção de dados inter-relacionados representando informações sobre um domínio específico;

IV – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos;

V – gestor negocial: responsável pela execução da atividade finalística no sistema ou conjunto de sistemas de TIC, bem como pela definição dos perfis de acesso dos usuários;

VI – gestor técnico: responsável pela sustentação de determinado sistema, conjunto de sistemas ou infraestrutura de TIC, bem como implementação do perfil de acesso ao usuário;

VII – log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

VIII – perfil de acesso: coleção de atributos e permissões que um usuário ou grupo de usuários têm no ambiente tecnológico;

IX – usuário: indivíduo que pode acessar informações, sistemas ou serviços do ambiente tecnológico;

X – usuários externos: magistrados, partes, advogados, membros do Ministério Público, visitantes e demais usuários que não estejam vinculados ao CNJ; e

XI – usuários internos: conselheiros, magistrados, servidores, estagiários, bem como colaboradores, prestadores de serviço, e demais usuários que estejam formalmente vinculados ao CNJ.

CAPÍTULO II

DA GESTÃO DOS RECURSOS DE TIC

Seção I

Da Central de Atendimento ao Usuário

Art. 3º As solicitações dos usuários para o uso de recursos de TIC do CNJ devem ser endereçadas à Central de Atendimento ao Usuário (CAU), utilizando os canais disponibilizados pelo DTI.

Parágrafo único. As solicitações dos usuários para o uso de recursos de TIC serão atendidas de acordo com a capacidade e infraestrutura do ambiente tecnológico do CNJ, bem como parâmetros e procedimentos estabelecidos pelo DTI.

Seção II

Dos Itens de Microinformática

Art. 4º Os equipamentos microcomputadores do tipo *desktop* ou *notebooks* são considerados itens de microinformática e deverão ser utilizados para fins exclusivamente laborais.

Art. 5º Os usuários internos poderão solicitar o empréstimo de itens de microinformática à CAU, estando sujeitos à análise da justificativa e à disponibilidade do item solicitado.

Parágrafo único: Usuários internos que estiverem em posse de itens de microinformática são inteiramente responsáveis por eventuais danos decorrente de mau uso e deverão observar ainda:

I – em viagens, acomodar os itens de microinformática, de forma segura, em mochilas, maletas, entre outros similares, e proceder o transporte como bagagem de mão;

II – em caso de roubo ou furto o usuário deverá registrar boletim de ocorrência perante as autoridades policiais locais e notificar imediatamente a CAU sobre o ocorrido; e

III – ao utilizar os itens de microinformática em hotéis, restaurantes, aeroportos, entre outros locais similares, evitar conectá-lo em redes públicas disponíveis.

Art. 6º Os itens de microinformática deverão obedecer aos seguintes requisitos de Segurança da Informação:

I – os perfis de acesso deverão ser aqueles com privilégios mínimos, estritamente necessários para o adequado desempenho das atividades laborais;

II – as atualizações de segurança do sistema operacional e demais *softwares* básicos deverão ser realizadas automaticamente, sob responsabilidade do DTI;

III – é obrigatória a utilização de *software* antivírus designado pelo DTI, bem como mantê-lo atualizado constantemente;

IV – os microcomputadores do tipo *notebook,* eventualmente utilizados fora das dependências físicas do CNJ, deverão utilizar solução criptográfica do tipo *Full-Disk Encryption* (FDE) provida pelo DTI, que ficará responsável por armazenar uma cópia da chave criptográfica utilizada;

V – caberá ao usuário bloquear a tela do microcomputador e de *notebooks* sempre que se ausentar do seu local de trabalho;

VI – o mecanismo de bloqueio automático de tela deverá ocorrer quando houver 10 (dez) minutos de inatividade do usuário;

VII – os mecanismos de hibernação e de suspensão deverão estar ativados e, caso isso não seja tecnicamente viável, microcomputadores e *notebooks* deverão ser desligados ao final do expediente pelo próprio usuário; e

VIII – a ligação na rede elétrica e o deslocamento dos microcomputadores do tipo *desktop* somente serão possíveis mediante acionamento da CAU.

Seção III

Dos *Softwares* de Terceiros

Art. 7º A instalação e a utilização de *softwares* de terceiros no ambiente tecnológico do CNJ estão sujeitas aos seguintes requisitos:

I – validação de segurança e potenciais vulnerabilidades, realizada por gestor técnico do DTI;

II – existência de licenças adquiridas pelo CNJ em quantidade suficiente para atender as demandas;

III – conformidade com as atividades de trabalho desenvolvidas pela unidade orgânica;

IV – compatibilidade com os demais *softwares* utilizados no ambiente tecnológico do CNJ; e

V – adequação aos recursos computacionais disponíveis.

§ 1º Os microcomputadores do tipo *desktop* e *notebook* disponibilizados pelo DTI conterão somente os *softwares* básicos, necessários para as atividades laborais dos usuários internos.

§ 2º A instalação de *softwares* complementares pode ser solicitada pelos usuários à CAU, estando sujeita à análise da justificativa e à disponibilidade das licenças.

§ 3º Cabe ao DTI manter atualizado o inventário de licenças de *softwares* utilizados no ambiente tecnológico do CNJ, bem como remover aqueles que porventura estejam instalados sem autorização devida.

Seção IV

Da Internet

Art. 8º Os usuários deverão utilizar o acesso à internet somente para fins laborais.

§ 1º Os registros de acesso à internet terão prazos de retenção definidos de acordo com a capacidade do ambiente tecnológico do CNJ e em conformidade com a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do CNJ.

Art. 9º É vedado aos usuários utilizar quaisquer serviços da internet para:

I – acessar conteúdo considerado ofensivo, ilegal, impróprio ou que infrinja direitos autorais;

II – acessar conteúdo que comprometa a segurança do ambiente tecnológico do CNJ;

III – baixar ou transferir (*download* ou *upload*) conteúdo multimídia (incluindo, por exemplo: imagens, vídeos, áudios), exceto para fins laborais;

IV – baixar ou transferir (*download* ou *upload*) jogos, scripts, códigos-fonte, programas de computador ou similares que não tenham sido expressamente autorizados pelo DTI;

V – utilizar serviços de compartilhamento de arquivos ou similares que não tenham sido expressamente autorizados pelo DTI; e

VI – realizar cadastro em redes sociais e serviços de mensagens instantâneas não autorizados, exceto quando a necessidade do serviço assim determinar.

Parágrafo único. O DTI poderá implementar mecanismos automatizados de controle de acesso, regulação de conteúdo e tráfego de rede de forma a preservar a segurança do ambiente tecnológico do CNJ.

Art. 10. A consulta ao registro de conteúdo de acesso à internet dos usuários poderá ser realizada pelo DTI quando houver decisão judicial ou com fulcro de assegurar a observância às regras desta Portaria, sendo esta última condicionada à abertura de processo administrativo de apuração de conduta.

Seção V

Do Correio eletrônico

Art. 11. O correio eletrônico (e-mail) institucional é instrumento formal utilizado pelos usuários do CNJ para comunicação, por meio de mensagens eletrônicas, para fins laborais.

§ 1º O DTI definirá os tipos permitidos e os tamanhos máximos dos arquivos que poderão ser anexados às mensagens eletrônicas, bem como os limites das caixas postais.

§ 2º Caberá ao usuário verificar periodicamente a sua caixa postal, eliminar as mensagens eletrônicas que não se façam mais necessárias e criar pastas locais no próprio microcomputador para armazenamento complementar, podendo, ainda, solicitar apoio à CAU.

§ 3º As caixas postais, bem como as mensagens, terão prazos de retenção definidos de acordo com a capacidade do ambiente tecnológico do CNJ e em conformidade com a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do CNJ.

§ 4º Os seguintes padrões de formação serão utilizados para os recursos do correio eletrônico:

I – As contas de usuário serão representadas no formato prenome.sobrenome@cnj.jus.br (em caso de coincidência de nomes, será adotado outro prenome ou sobrenome a ser definido pelo usuário em conjunto com a CAU);

II – As caixas postais para atendimento das unidades orgânicas do CNJ serão representadas no formato sigladaunidade@cnj.jus.br;

III – As caixas postais para atender necessidades especiais das unidades orgânicas do CNJ serão representadas no formato assunto@cnj.jus.br;

IV – Os grupos de distribuição serão representados no formato g-nome1.nome2@cnj.jus.br; e

V – As listas de discussão serão representadas no formato assuntodiscutido@listas.cnj.jus.br.

Art. 12. As listas de discussão serão utilizadas exclusivamente para troca de mensagens e informações entre os usuários internos e externos sobre assuntos de interesse do CNJ.

Parágrafo único. Ao requisitar a criação de uma lista de discussão para evento específico, o gestor negocial deverá informar o período de utilização, o nome do responsável pelo acompanhamento e pela moderação dos assuntos que serão tratados, bem como a definição de inclusão ou exclusão dos usuários da lista.

Art. 13. É vedado o uso do correio eletrônico para:

I – fins particulares, comerciais e políticos ou como meio para prática de crimes;

II – transmitir ou acessar conteúdo que comprometa a segurança do ambiente tecnológico do CNJ;

III – transmitir ou acessar conteúdo lascivo, preconceituoso, discriminatório, calunioso, ilegal ou qualquer outro tipo que atente contra a honra, a moral e aos bons costumes;

IV – propagar *softwares* maliciosos, realizar ataques de engenharia social ou qualquer outro tipo de ataque cibernético;

V – transmitir mensagens não solicitadas para grande número de pessoas (spam); e

VI – realizar ações ilegais, impróprias, ou que infrinjam direitos autorais.

Parágrafo único. O DTI poderá implementar mecanismos automatizados de controle das mensagens de forma a preservar a segurança do ambiente tecnológico do CNJ.

Art. 14. O conteúdo das mensagens eletrônicas poderá ser acessado pelo DTI quando houver decisão judicial ou com fulcro de assegurar a observância às regras desta Portaria, sendo esta última condicionada à abertura de processo administrativo de apuração de conduta.

Seção VI

Do armazenamento de arquivos

Art. 15. Cada usuário ou unidade orgânica do CNJ poderá dispor de uma área para armazenamento exclusivo de arquivos para fins laborais.

§ 1º O DTI estabelecerá os padrões, tipos, limites e os meios de armazenamento de arquivos de acordo com a capacidade do ambiente tecnológico do CNJ.

§ 2º Os usuários ou unidades orgânicas poderão compartilhar arquivos de sua área de armazenamento, respeitando as disposições previstas em lei e demais regulamentos quanto à classificação e ao tratamento da informação.

§ 4º As áreas de armazenamento terão prazos de retenção definidos de acordo com a capacidade do ambiente tecnológico do CNJ e em conformidade com a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do CNJ.

Art. 16. É vedado utilizar as áreas de armazenamento para arquivos de:

I – conteúdo considerado ofensivo, ilegal, impróprio ou que infrinja direitos autorais;

II – multimídia (incluindo, por exemplo: imagens, vídeos, áudios), exceto para fins laborais;

III – jogos, *scripts*, códigos-fonte, programas de computador ou similares, que não tenham sido expressamente autorizados pelo DTI; e

IV – quaisquer outros tipos que não tenham fins laborais, inclusive arquivos pessoais.

Parágrafo único. O DTI poderá implementar mecanismos automatizados de controle do armazenamento de arquivos de forma a preservar a segurança do ambiente tecnológico do CNJ.

Art. 17. O DTI poderá acessar o conteúdo dos arquivos que estejam em área de armazenamento de usuários ou unidades orgânicas quando houver decisão judicial ou com fulcro de assegurar a observância às regras desta Portaria, sendo esta última condicionada à abertura de processo administrativo de apuração de conduta.

Seção VII

Dos dispositivos de impressão

Art. 18. Os recursos (impressoras e insumos) necessários para o provimento de impressão de documentos no ambiente do CNJ deverão ser utilizados para fins laborais e deverão estar aderentes às diretrizes estabelecidas no Plano de Logística Sustentável (PLS) do CNJ.

Art. 19. Os equipamentos de impressão deverão ser utilizados de forma compartilhada pelos usuários da unidade orgânica, observando os seguintes preceitos:

I – possuir mecanismo de impressão frente e verso, além da possibilidade de serem conectados diretamente na rede de computadores para maximização da economia e sustentabilidade ambiental; e

II – a impressão em lado único da folha de papel e de documentos em cores deverá ser entendida como de excepcional necessidade, de forma a evitar o uso desnecessário de recursos.

Parágrafo único. Visando estimular o cumprimento das metas do PLS, a Administração poderá recomendar que o DTI estabeleça quota ou limite de impressão por unidade orgânica ou usuário.

Seção VIII

Do repositório de dados e dos bancos de dados

Art. 20. O acesso ao repositório de dados ou ao banco de dados dos sistemas do ambiente tecnológico do CNJ será gerenciado pelo gestor técnico designado pelo DTI.

Parágrafo único. O direito de acesso aos repositórios de dados ou aos bancos de dados em quaisquer ambientes (desenvolvimento, homologação, teste, sustentação, produção etc.) somente ocorrerá após autorização do gestor negocial que deverá informar o perfil de acesso em relação aos dados.

Art. 21. A mudança de definição ou na arquitetura de infraestrutura de armazenamento de dados ou de banco de dados dos sistemas do ambiente tecnológico do CNJ será gerenciado pelo gestor técnico designado pelo DTI.

Parágrafo único. A mudança referida no caput ou a migração de dados em quaisquer ambientes (desenvolvimento, homologação, teste, sustentação, produção etc.) somente ocorrerá após autorização do diretor técnico do DTI ou por sua delegação.

Art. 22. O envio de informações extraídas dos repositórios de dados ou dos bancos de dados do ambiente tecnológico do CNJ para ambiente externo somente ocorrerá após análise do gestor negocial e posterior autorização do diretor técnico do DTI ou por sua delegação.

Parágrafo único. Para evitar a exposição de dados sigilosos, o gestor técnico irá aplicar, quando possível, regras de mascaramento de dados, criptografia ou qualquer outro procedimento técnico que assegure o princípio da confidencialidade dos dados considerados sensíveis pelo gestor negocial, em total observância à Lei Geral de Proteção de Dados (LGPD).

Seção IX

Do monitoramento e auditoria do ambiente tecnológico

Art. 23. O DTI realizará o monitoramento permanente da atividade cibernética do ambiente tecnológico do CNJ para fins de segurança e auditoria.

Parágrafo único. O monitoramento referido no caput não possui a finalidade de coletar informações que infrinjam o direito à intimidade, à vida privada, à honra e à imagem dos usuários.

Art. 24. As ações praticadas por usuários e sistemas autônomos deverão ser encaminhadas para um serviço centralizado de registro de eventos (*logs*), de modo que seja possível identificar:

I – quem executou determinada ação;

II – quais ações foram executadas;

III – quando as ações foram executadas; e

IV – em qual ativo de informação as ações foram executadas.

Art. 25. O registro dos eventos (*logs*) — para fins de segurança e auditoria — terá prazos de retenção definidos de acordo com a capacidade do ambiente tecnológico do CNJ e em conformidade com a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do CNJ, não podendo ser inferior a:

I – 180 (cento e oitenta) dias para serviços críticos; e

II – 90 (noventa) dias para os demais serviços.

CAPÍTULO III

DAS DISPOSIÇÕES FINAIS

Art. 26. Ficam reservados os seguintes períodos: das 20h das quintas-feiras às 8h das sextas-feiras; e das 20h das sextas-feiras às 8h das segundas-feiras, além dos horários definidos em normativos específicos para manutenções preventivas e corretivas dos sistemas de informação, bem como dos ativos de infraestrutura de TIC.

§ 1º A paralisação temporária programada ou emergencial de um sistema de informação deverá ocorrer por meio de comunicado aos usuários do CNJ, a ser emitido pelo DTI, com até 48 horas de antecedência.

§ 2º Em situações excepcionais poderão ser efetuadas manutenções técnicas emergenciais em outros dias e horários, além dos previstos, com o devido comunicado aos usuários do CNJ, a ser emitido pelo DTI.

§ 3º É vedada a manutenção preventiva/corretiva no dia anterior e no mesmo dia de Sessão Plenária do CNJ, salvo sob autorização do diretor técnico do DTI ou por sua delegação.

Art. 27. O uso inapropriado dos recursos pelos usuários é passível de apuração de responsabilidade, nos termos da legislação aplicável, podendo o DTI suspender imediatamente o acesso concedido.

Parágrafo único. A suspensão será comunicada pelo DTI para o usuário e, quando for caso, também para o titular da unidade orgânica a qual o usuário é associado, esclarecendo os detalhes da ocorrência.

Art. 28. A inobservância dos dispositivos constantes desta Portaria pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 29. As situações não previstas nesta Portaria deverão ser resolvidas pelo Comitê de Governança de Tecnologia da Informação e Comunicação.

Art. 30. Esta Portaria deverá ser revisada bianualmente ou quando necessário.

Art. 31. Ficam revogadas:

I – a Instrução Normativa nº 51, de 4 de julho de 2013; e

II – a Instrução Normativa nº 54, de 12 de novembro de 2013.

Art. 32. Esta Portaria entra em vigor 180 (cento e oitenta) dias após a sua publicação.

Ministro **Luís Roberto Barroso**