RESOLUÇÃO N.º 23-TJ, DE 21 DE AGOSTO DE 2019

Regulamenta a Política de Segurança da Informação (PSI) do Poder Judiciário do Estado do Rio Grande do Norte

O TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO NORTE, no uso das suas atribuições legais, e tendo em vista o que foi deliberado na Sessão Plenária desta data,

CONSIDERANDO que todos têm o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado, nos termos do inciso XXXIII do art. 5º da Constituição Federal;

CONSIDERANDO que é dever de todo agente público prestar as informações requeridas pelo público em geral, ressalvadas as protegidas por sigilo, bem como guardar sigilo sobre assuntos institucionais, nos termos do art. 116 da Lei nº 8.112, de 11 de dezembro de 1990;

CONSIDERANDO a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, instituída por meio do Decreto nº 3.505, de 13 de junho de 2000;

CONSIDERANDO as disposições contidas no Decreto nº 4.553, de 27 de dezembro de 2002, que dispõem sobre a salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam;

CONSIDERANDO que o conjunto de dados, informações, conhecimentos, agentes públicos e recursos físicos existentes no âmbito do Tribunal de Justiça do Rio Grande do Norte são essenciais ao cumprimento de sua missão institucional e requerem a adoção de medidas especiais de segurança, devido à importância estratégica de suas ações para a defesa dos interesses nacionais e a segurança da sociedade e do Estado; e

CONSIDERANDO, finalmente, a legislação pertinente à matéria, notadamente a Lei nº 8.112/1990, a Lei nº 8.159/1991, a Lei nº 9.983/2000, o Decreto nº 3.505/2000, o Decreto nº 4.553/2002, o Decreto nº 5.482/2005, o Decreto nº 6.029/2007, o Decreto nº 6.932/2009 e, ainda, a Instrução Normativa GSI nº 1/2008, a Norma Complementar nº 03/IN01/DSIC/GSIPR, de 10 de junho de 2009, a Norma Complementar nº 04/IN01/DSIC/GSICPR, de 14 de agosto de 2009, a Resolução nº 104/2010 do CNJ, a Norma Complementar nº 05/IN01/DSIC/GSICPR, de 14 de agosto de 2009, e Normas ABNT NBR ISO/IEC 27001 e 27002, que institui o código de melhores práticas para gestão da segurança da informação;

RESOLVE:

Art. 1º A Política de Segurança da Informação (PSI) do Poder Judiciário do Estado do Rio Grande do Norte (PJRN) é regida pela presente Resolução e se aplica a todas as suas unidades.

Art. 2º A PSI, como parte das diretrizes estratégicas do PJRN, objetiva instituir responsabilidades e competências, visando garantir a segurança das informações, dos agentes públicos e das estruturas físicas das unidades judiciárias.

Art. 3º Para os efeitos desta Resolução, consideram-se:

I - agente público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao PJRN;

II - ativo: aquilo que tem valor tangível ou intangível para o PJRN, tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional;

III - autenticidade: propriedade que assevera que os dados ou informações são verdadeiros e fidedignos tanto na origem quanto no destino, permitindo, inclusive, a identificação do emissor e do equipamento utilizado, quando for o caso;

IV - central de serviços agile - sistema onde os usuários do PJRN devem, exclusivamente, efetuar solicitações relacionadas à Tecnologia da Informação e Comunicação (TIC);

V - Comitê de Segurança da Informação (CSI): grupo responsável pelo desenvolvimento, aplicação, atualização e divulgação das políticas de segurança da informação do PJRN;

VI - confidencialidade: propriedade que garante acesso à informação somente às pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizados não tenham conhecimento da informação, de forma proposital ou acidental;

VII - conformidade: propriedade que garante que um processo siga as leis e regulamentos aplicáveis;

VIII - criticidade: grau de importância do ativo para a continuidade das atividades e serviços do PJRN;

IX - descarte seguro: eliminação correta de informações, documentos, mídias e acervos digitais;

X - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XI - incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação de sistemas de computação ou das redes de computadores;

XII - integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representa a fidedignidade da informação;

XIII - não repúdio: propriedade que impossibilita a negação da autoria de uma ação;

XIV - demandas excepcionais: procedimentos de intervenção direta na base de dados ou aos sistemas, que envolvam a segurança da informação dos recursos de TIC e não possam ser executados sob responsabilidade do usuário;

XV - segurança da informação: proteção contra ameaças para garantir a confidencialidade, disponibilidade, integridade e autenticidade das informações;

XVI - usuário externo: qualquer pessoa física ou jurídica que tenha acesso, mediante autorização quando cabível, a informações produzidas e aos serviços fornecidos pelo PJRN e qualquer pessoa física que não se caracterize como usuário interno;

XVII - usuário interno: qualquer magistrado, agente, prestador de serviço, estagiário ou colaborador que necessite de acesso, de forma autorizada, ao uso dos recursos de TIC e às informações privadas ou sigilosas do PJRN;

XVIII - usuário: conjunto formado por usuário interno e usuário externo, conforme incisos XVI e XVII;

XIX - conta de sistema: qualquer conta disponibilizada pela SETIC para acesso à rede por sistemas, serviços e dispositivos a órgãos ou empresas.

Art. 4º A Política de Segurança da Informação (PSI) tem por objetivo geral estabelecer as diretrizes e o apoio necessários para assegurar o sigilo, a integridade, a autenticidade e a disponibilidade de dados, informações e conhecimentos no âmbito do PJRN, bem como promover a proteção dos agentes públicos e dos ativos da Instituição, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais.

Art. 5º São objetivos específicos da Política de Segurança da Informação (PSI):
I - dotar o PJRN de instrumentos normativos e organizacionais necessários ao efetivo desenvolvimento, aplicação e atualização da PSI;
II - orientar a adoção de mecanismos, medidas e procedimentos de proteção a dados, informações e conhecimentos relativos à privacidade das pessoas, ao interesse institucional e aos direitos de propriedade intelectual;
III - nortear a adoção de mecanismos, medidas e procedimentos internos para que o acesso a dados e informações sensíveis e sigilosos seja permitido apenas às pessoas e órgãos autorizados, segundo a legislação vigente;
IV - subsidiar ações voltadas à salvaguarda da exatidão e integridade de dados, informações e conhecimentos, bem como dos métodos de trabalho;
V - direcionar a adoção de medidas que assegurem a disponibilidade de dados, informações, conhecimentos e ativos associados às pessoas e órgãos autorizados;
VI - orientar as ações permanentes de conscientização, capacitação e educação sobre a importância da proteção de dados, informações e conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação;
VII - nortear as ações necessárias à proteção dos agentes públicos e demais ativos do PJRN;
VIII - apontar responsáveis pela aplicação e garantia do cumprimento da PSI;
IX - estabelecer ou referenciar sanções em caso de não cumprimento das normas de segurança;
X - nortear classificações de informações e de ativos de TI no âmbito do PJRN; e
XI - estabelecer critérios para classificação de soluções tecnológicas como estratégicas e não estratégicas.

Art. 6º Além dos princípios aplicáveis à Administração Pública em geral, a aplicação e o cumprimento da Política de Segurança da Informação (PSI) atenderão às regras de sigilo e aos princípios de integridade, disponibilidade e autenticidade.

Art. 7º São diretrizes da Política de Segurança da Informação (PSI):
I - o desenvolvimento de sistema de classificação de dados, informações e conhecimentos, com o objetivo de garantir os níveis de segurança desejados;
II - a utilização de critérios adequados, segundo a necessidade de conhecer, na classificação de documentos e recursos físicos;
III - a definição de procedimentos e níveis de acesso a dados, informações e conhecimentos no âmbito do PJRN, segundo a necessidade de conhecer e, quando for o caso, mediante credencial de segurança;
IV – o estabelecimento de normas, padrões e procedimentos relacionados à produção, tramitação, transporte, manuseio, custódia, armazenamento, conservação e eliminação de dados, informações e materiais no âmbito do PJRN;
V - a adoção de critérios e procedimentos relacionados ao uso dos recursos de TIC no âmbito do PJRN;
VI - o estabelecimento e o aprimoramento de critérios, medidas e procedimentos de seleção, ingresso, desempenho na função, movimentação ou desligamento de agentes públicos no âmbito do PJRN, mediante a implementação e a atualização de um sistema de informações;
VII - a garantia de que todos os privilégios de acesso a ativos e recursos físicos do PJRN sejam devidamente revistos, modificados ou revogados quando alteradas ou cessadas as atividades do agente público junto a este Poder;
VIII - o estabelecimento de normas, padrões e procedimentos necessários ao controle de acesso e à proteção dos agentes públicos e demais ativos do PJRN;
IX - o estabelecimento de normas relativas ao desenvolvimento, à manutenção e ao monitoramento dos sistemas de informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados;
X - a conformidade dos processos de aquisição de bens e serviços com os preceitos legais e os princípios de segurança da informação;
XI - o desenvolvimento e a implantação de programas de conscientização e capacitação sobre segurança da informação;

XII - o desenvolvimento e a execução de planos de contingência;

XIII - o estabelecimento de medidas e procedimentos de proteção contra falhas e danos que possam comprometer as atribuições do PJRN;

XIV - o estabelecimento de um Plano de Continuidade de Negócio (PCN) para diminuir o tempo de indisponibilidade face algum incidente de segurança; e

XV - estabelecimento de modelos base para o Termos de Aceite, Termo de Responsabilidade e para o Termo de Manutenção de Sigilo do PJRN.

Art. 8º O acesso a dados, informações, conhecimentos e recursos físicos deve ser estabelecido segundo as necessidades indispensáveis e inerentes ao cumprimento do dever funcional.
Parágrafo único. O acesso a dados, informações e conhecimentos sensíveis e sigilosos dar-se-á segundo a necessidade de conhecer e, quando for o caso, mediante credencial de segurança.

Art. 9º As demandas excepcionais que reúnem as diretrizes referentes aos procedimentos de acesso direto ao banco de dados e/ou aos sistemas (art.3º, inciso XIV), devem ser formalizadas exclusivamente a partir do

preenchimento do formulário disponibilizado na intranet do TJRN, no Agile Web, em: https://agile.tjrn.jus.br/ ou diretamente no endereço https://apps.tjrn.jus.br/demex/, acessível somente aos Magistrados e seus Assessores e Secretários do Tribunal. A solicitação será encaminhada ao Núcleo de Governança Estratégica (Resolução nº 01/2017-TJ) que, após analisar e emitir parecer, encaminhará à Secretaria de Tecnologia da Informação e Comunicação (SETIC), para autorizar ou não sua execução.

Art. 10. Além da classificação estabelecida na legislação vigente, com relação à salvaguarda de dados, informações, documentos e materiais sigilosos, deve ser adotada classificação institucional, a ser regulamentada em ato próprio, segundo o grau de sensibilidade dos dados, informações, documentos e recursos físicos.

Art. 11. A utilização dos recursos de TIC do PJRN, por parte de Órgãos e entidades externas, deverá obedecer às seguintes diretrizes:

I - para os casos de necessidade de utilização de equipamento de TIC de outro Órgão nas dependências do PJRN, este equipamento deverá:

a) ser homologado pela equipe técnica da SETIC;
b) ingressar no domínio da rede corporativa do PJRN;
c) utilizar credenciais de acesso fornecidas pela SETIC, seguindo o Princípio do Privilégio Mínimo;
d) adotar os controles de segurança de informação utilizados pela SETIC;

II - em eventual necessidade de acesso à rede Wi-Fi Corporativa do PJRN, que se dará através da obediência ao Princípio do Privilégio;

III – nos casos de necessidade de conexão ou compartilhamento das bases de dados do PJRN, deverá ser firmado Termo de Cooperação Técnica e específico, contendo, no mínimo, os seguintes pontos:

a) detalhamento da base de dados, tabelas e campos a serem acessados pelo Órgão parceiro;
b) especificações técnicas do Sistema Gerenciador de Banco de Dados - SGBD utilizado pela instituição parceira;
c) observância às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário;
d) definição do método de conexão entre o TJRN e a instituição parceira;
e) respeito integral à Política de Segurança da Informação do PJRN;

Art. 12. Compete ao Comitê de Segurança Institucional (CSI) garantir o desenvolvimento, a aplicação e a atualização da Política de Segurança da Informação (PSI) do PJRN, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

Art. 13. Cabe aos gestores das demais unidades que compõem a estrutura organizacional do PJRN dar cumprimento à Política de Segurança da Informação (PSI) no âmbito de suas respectivas atribuições, garantir, por parte dos colaboradores do seu setor, o conhecimento das orientações do CSI relacionadas à PSI.

Art. 14. O CSI deve orientar e assistir às demais unidades organizacionais do PJRN em questões de segurança da informação relativas às atividades da Justiça Estadual.

Art. 15. O descumprimento da PSI, bem como das normas e dos procedimentos dela decorrentes, acarretará a responsabilização administrativa, civil e criminal por desvios éticos e morais cometidos.

Art. 16. O CSI, em conjunto com as demais unidades da estrutura organizacional do PJRN, promoverá a comunicação e a ampla divulgação da PSI para ciência e cumprimento de todos, no âmbito de suas atribuições.

Art. 17. A PSI deve ser aplicada no âmbito do PJRN, segundo as prioridades identificadas pelo CSI, e a todas as suas unidades organizacionais, inclusive àquelas localizadas em outros municípios, respeitando-se suas especificidades.
Parágrafo único. Normas de segurança da informação específicas poderão ser elaboradas e estabelecidas em conjunto com os demais interessados, quando um setor do Poder Judiciário do Estado do Rio Grande do Norte estiver instalado em prédios não destinados exclusivamente às suas atividades, desde que as normas sejam compatíveis com a PSI e com as estratégias de negócio do PJRN.

Art. 18. O PJRN exigirá dos agentes públicos Termo de Manutenção de Sigilo de não divulgação de dados, informações e conhecimentos sigilosos ou sensíveis a que, direta ou indiretamente, tenham acesso no exercício de cargos, funções ou empregos públicos, mesmo após lotação, afastamento definitivo ou temporário do colaborador.
§ 1º As empresas terceirizadas ou quaisquer entidades que disponibilizem pessoal para exercer atividades junto ao PJRN deverão garantir a adoção das medidas previstas neste artigo.
§ 2º O Termo de Manutenção de Sigilo valerá mesmo após o término do contrato com a empresa terceirizada ou do término do vínculo do colaborador com sua contratante.

Art. 19. A PSI deve ser aplicada, no que couber, a terceiros contratados ou conveniados.

Art. 20. O CSI, com a colaboração das demais unidades organizacionais do TJRN, estabelecerá mediante Portaria os critérios e os indicadores para o monitoramento e a avaliação da eficácia, da eficiência e da efetividade da PSI.

Art. 21. A PSI deve ser revisada e atualizada periodicamente, no máximo, a cada dois anos.
Parágrafo único. O processo de revisão é de responsabilidade do CSI que irá analisar criticamente as diretrizes da PSI, avaliando sua aplicabilidade e alinhamento com os objetivos do PJRN.

Art. 22. As dúvidas e os casos omissos serão dirimidos pelo CSI e, em última instância, pela Presidência do Tribunal de Justiça do Rio Grande do Norte, segundo os

objetivos, os princípios e as diretrizes estabelecidos nesta Resolução.

Art. 23. A Presidência do Tribunal de Justiça do Estado do Rio Grande do Norte expedirá Atos específicos sobre as normas de segurança da informação de cada área, observadas as diretrizes da presente Resolução.

Art. 24. As situações tratadas pela Resolução Nº 013/2012-TJ, não se inserem nos conceitos, definições e dispositivos desta Resolução.

Art. 25. Fica revogada a Resolução n° 023/2017-TJ, de 23 de Maio de 2017.

Art. 26. Esta Resolução entra em vigor na data de sua publicação.

Sala das Sessões do Tribunal Pleno “Desembargador João Vicente da Costa”, em Natal, 21 de agosto de 2019.

DES. JOÃO REBOUÇAS
PRESIDENTE

DES. CLAUDIO SANTOS

DES. EXPEDITO FERREIRA

DES. VIVALDO PINHEIRO

DES. AMÍLCAR MAIA

DES.ª MARIA ZENEIDE BEZERRA

DES. IBANEZ MONTEIRO

DES. GLAUBER RÊGO

DES. GILSON BARBOSA

DES. CORNÉLIO ALVES