CONSELHO NACIONAL DE JUSTIÇA
PRESIDÊNCIA

RESOLUÇÃO Nº 396, DE 7 DE JUNHO DE 2021.

Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO que compete ao CNJ a atribuição de coordenar o planejamento e a gestão estratégica de Tecnologia da Informação e Comunicação (TIC) do Poder Judiciário;

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro;

CONSIDERANDO os termos da Resolução CNJ nº 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e estabelece as diretrizes para sua governança, gestão e infraestrutura;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;

CONSIDERANDO o que dispõe a Lei nº 13.709/2018, com a redação dada pela Lei nº 13.853/2019, sobre a proteção de dados pessoais, que altera a Lei nº 12.965/2014 (Marco Civil da Internet);

CONSIDERANDO o disposto na Resolução CNJ nº 291/2019, que instituiu o Sistema Nacional de Segurança do Poder Judiciário;

CONSIDERANDO o disposto na Portaria CNJ nº 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO o disposto na Portaria CNJ nº 249/2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

CONSIDERANDO que, para contemplar aspectos fundamentais para o desenvolvimento da Política sobre a área da Segurança Cibernética, será necessário abordar aspectos da Segurança da Informação, área sistêmica e mais abrangente,

Fonte: Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 149, p. 2-8, 10 jun. 2021.

CONSIDERANDO a deliberação do Plenário do CNJ no Ato Normativo nº **0003201-92.2021.2.00.0000**, na 87ª Sessão Virtual, realizada em 28 de maio de 2021;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Instituir a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito dos órgãos do Poder Judiciário, à exceção do Supremo Tribunal Federal (STF).

Parágrafo único. A ENSEC-PJ prevista nesta Resolução contempla:

I – temas relacionados à segurança da informação, de forma ampla, que sejam essenciais para segurança cibernética;

II – segurança física e proteção de dados pessoais e institucionais, nos aspectos relacionados à cibersegurança;

III – segurança física e proteção de ativos de tecnologia da informação de forma geral;

IV – ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;

V – ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades fim e administrativas dos órgãos do Poder Judiciário;

VI – ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética;

VII – ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética; e

VIII – ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de tecnologia da informação e comunicação que atuam na área de segurança cibernética.

CAPÍTULO II
OBJETIVOS DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ENSEC-PJ)

Art. 2º A ENSEC-PJ tem o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário, abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito.

Art. 3º Para a concretização dos objetivos da segurança cibernética instituídos na Política de Segurança Cibernética do Poder Judiciário (PSEC-PJ), estrutura-se a presente Estratégia Nacional de Segurança Cibernética com visão, objetivos e ações capazes de conduzir os órgãos do Poder Judiciário a um ambiente desenvolvido, resistente e seguro.

CAPÍTULO III
DA VISÃO, DOS OBJETIVOS E DAS AÇÕES

Art. 4º A visão da ENSEC-PJ consiste em alcançar a excelência em segurança cibernética no Poder Judiciário.

Art. 5º Os objetivos da ENSEC-PJ são a base para tornar o espaço cibernético mais confiável, resistente, inclusivo e seguro e visam direcionar as ações dos órgãos do Poder Judiciário na área de segurança cibernética.

Art. 6º São objetivos da ENSEC-PJ:

I – tornar o Judiciário mais seguro e inclusivo no ambiente digital;

II – aumentar a resiliência às ameaças cibernéticas;

III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e

IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Art. 7º As ações da ENSEC-PJ foram estabelecidas com a finalidade de possibilitar o alcance dos objetivos e basearam-se no estágio de maturidade geral dos órgãos do Poder Judiciário.

Art. 8º Os órgãos do Poder Judiciário, com exceção do STF, devem colocar em prática as ações para o pleno alcance dos objetivos da ENSEC-PJ.

Parágrafo único. O engajamento da alta administração de cada tribunal é essencial para a consecução das finalidades e das medidas de proteção ao serviço, sobretudo quando implicarem a necessidade de rápida suspensão do acesso ao público, para evitar o alastramento de ataque cibernético e conter os danos.

Art. 9º São ações da ENSEC-PJ:

I – fortalecer as ações de governança cibernética;

II – elevar o nível de segurança das infraestruturas críticas;

III – estabelecer rede de cooperação do Judiciário para a segurança cibernética; e

IV – estabelecer modelo centralizado de governança cibernética nacional.

Art. 10. Para fortalecer as ações de governança cibernética, deve-se estabelecer um Sistema de Gestão em Segurança da Informação baseado em riscos, de acordo com recomendação do CNJ.

Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:

I – estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão;

II – instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR);

III – elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa;

IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários,

permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança;

V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da *internet*;

VI – providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes;

VII – elaborar requisitos específicos de segurança cibernética relativos aos ativos sob sua jurisdição, incluindo ambientes centralizados, *endpoints*, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares;

VIII – elaborar requisitos específicos de segurança cibernética relacionados com o trabalho remoto;

IX – adotar práticas e requisitos de segurança cibernética no desenvolvimento de novos projetos, tais como dupla verificação do acesso externo;

X – realizar, ao menos semestralmente, avaliação e testes de conformidade em segurança cibernética de forma a aferir a eficácia dos controles estabelecidos;

XI realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo; e

XII – estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado com objetivo colaborativo.

CAPÍTULO IV
DO MODELO CENTRALIZADO DE GOVERNANÇA NACIONAL NA SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

Art. 12. O modelo centralizado de governança nacional na segurança cibernética do Poder Judiciário tem os seguintes objetivos:

I – promover a coordenação dos diversos entes relacionados com a segurança cibernética;

II – possibilitar a análise conjunta do nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário;

III – estabelecer e desenvolver padrão de maturidade unificado de segurança cibernética, de forma que seja possível avaliar o nível de maturidade de cada órgão do Judiciário, por meio de indicadores estabelecidos;

IV – estabelecer rotinas de verificações de conformidade em segurança cibernética; e

V – possibilitar a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança cibernética.

Art. 13. O CNJ coordenará as ações para viabilizar a governança nacional em segurança cibernética do Poder Judiciário.

CAPÍTULO V
DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO PODER JUDICIÁRIO

Art. 14. Fica instituído o Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ), com atribuição de assessorar o CNJ nas atividades relacionadas

à segurança da informação.

Art. 15. Integram o CGSI-PJ:
I – dois especialistas representantes do Conselho Nacional de Justiça;
II – dois especialistas representantes do Supremo Tribunal Federal;
III – um especialista representante do Superior Tribunal de Justiça;
IV – um especialista representante do Tribunal Superior Eleitoral;
V – um especialista representante do Tribunal Superior do Trabalho;
VI – um especialista representante do Conselho Superior da Justiça do Trabalho;
VII - um especialista representante do Conselho da Justiça Federal;
VIII – um especialista representante do Superior Tribunal Militar; e
IX – dois especialistas representantes dos Tribunais de Justiça Estaduais.

§ 1º O CGSI-PJ será coordenado por um representante do Conselho Nacional de Justiça designado pela Presidência.

§ 2º As indicações dos representantes dos incisos I e IX serão feitas pela Presidência do CNJ.

§ 3º O CGSI-PJ poderá convidar representantes de órgãos de segurança pública, do Ministério Público, das Forças Armadas e especialistas técnicos de outros órgãos públicos ou privados que pretendam subsidiar os respectivos trabalhos.

§ 4º Os integrantes do CGSI-PJ deverão ter conhecimento técnico na área de segurança da informação.

Art. 16. O CGSI-PJ se reunirá, em caráter ordinário, semestralmente, e, em caráter extraordinário, por convocação de seu coordenador.

Art. 17. Compete ao CGSI-PJ, assessorando o CNJ, nos temas relacionados à segurança da informação:
I – estabelecer norma sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação no Poder Judiciário;
II – aprovar políticas, diretrizes, estratégias, normas e recomendações relacionadas à segurança da informação no Poder Judiciário;
III – elaborar e implementar programas sobre segurança da informação destinados à conscientização e à capacitação dos servidores do Poder Judiciário;
IV – estabelecer critérios que permitam monitorar e avaliar a execução da PSEC-PJ e de seus instrumentos, bem como o nível de maturidade em segurança da informação em cada órgão do Poder Judiciário;
V – estabelecer norma de criação e funcionamento do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), que funcionará como canal oficial de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos; e
VI – promover troca de informações e experiências com os comitês gestores de segurança da informação dos outros Poderes e com a sociedade.

CAPÍTULO VI
DA REDE NACIONAL DE COOPERAÇÃO DO PODER JUDICIÁRIO NA ÁREA DE SEGURANÇA CIBERNÉTICA

Art. 18. A Rede de Cooperação do Judiciário na área de segurança cibernética tem os seguintes objetivos:

I – promover ambiente participativo, colaborativo e seguro entre os órgãos do Poder Judiciário, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos;

II – estimular o compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticas;

III – realizar exercícios cibernéticos com a participação de múltiplos entes;

IV – fortalecer o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CPTRIC-PJ) do CNJ;

V – aperfeiçoar a estrutura judiciária para o aprimoramento de investigações de crimes cibernéticos;

VI – incentivar a criação e a atuação de ETIR em cada órgão do Poder Judiciário;

VII – emitir alertas e recomendações de segurança cibernética; e

VIII – ampliar parceria com outros órgãos do Poder Executivo, do Poder Legislativo, do Ministério Público, da polícia judiciária, do setor privado e do meio acadêmico, com vistas a elevar, de modo geral, o nível de segurança cibernética.

Parágrafo único. Para fins de cumprimento dos objetivos estabelecidos, todos os órgãos do Judiciário que detectarem incidentes de segurança cibernética deverão reportá-los ao CPTRIC-PJ.

Art. 19. Compete à alta administração dos órgãos do Poder Judiciário, com exceção do STF, realizar a governança da segurança da informação e especialmente:

I – implementar, no que lhe couber, a Política de Segurança Cibernética do Poder Judiciário;

II – elaborar a Política de Segurança da Informação e normas internas correlatas ao tema, observadas as normas de segurança da informação editadas pelo CNJ;

III – destinar recursos orçamentários específicos para as ações de segurança da informação;

IV – promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

V – instituir e implementar ETIR, que comporá a rede de equipes vinculadas ao CPTRIC-PJ;

VI – coordenar e executar as ações de segurança da informação no âmbito de sua atuação; e

VII – aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.

Art. 20. Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir CGSI, ao qual caberá:

I – assessorar a alta administração do órgão do Poder Judiciário em todas as questões relacionadas à segurança da informação;

II – propor alterações na política de segurança da informação e deliberar sobre assuntos a ela relacionados, incluindo atividades de priorização de ações e gestão de riscos de segurança;

III – propor normas internas relativas à segurança da informação;

IV – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação; e

V – consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.

§ 1º O CGSI será coordenado pela autoridade responsável pela segurança da informação no respectivo órgão do Poder Judiciário, nomeado por seu presidente.

§ 2º Os órgãos do Poder Judiciário, com exceção do STF, editarão atos para definir a forma de funcionamento dos respectivos CGSIs, observado o disposto nesta Resolução e na legislação de regência.

Art. 21. Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC.

§ 1º O titular da estrutura prevista no *caput* deste artigo será o gestor de segurança da informação do órgão.

§ 2º O gestor de segurança da informação terá as seguintes atribuições:

I – instituir e gerir o Sistema de Gestão de Segurança da Informação;

II – implementar controles internos fundamentados na gestão de riscos da segurança da informação;

III – planejar a execução de programas, de projetos e de processos relativos à segurança da informação com as demais unidades do órgão;

IV – implantar procedimento de tratamento e resposta a incidentes em segurança da informação; e

V – observar as normas e os procedimentos específicos aplicáveis em consonância com os princípios e as diretrizes desta Resolução e da legislação de regência.

CAPÍTULO VII
DA POLÍTICA DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

Art. 22. A PSEC-PJ tem a finalidade de prover os princípios, objetivos e instrumentos capazes de assegurar a Segurança Cibernética no Poder Judiciário.

Art. 23. São princípios da PSEC-PJ:

I – segurança jurídica;

II – respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção de privacidade e o acesso à informação;

III – visão abrangente e sistêmica da segurança cibernética;

IV – integração, cooperação e intercâmbio científico e tecnológico relacionado à segurança cibernética entre os órgãos da Administração Pública Federal e do meio acadêmico;

V – educação e inovação como alicerce fundamental para o fomento da cultura em segurança cibernética;

VI – orientação à gestão de riscos e à gestão da segurança da informação;

VII – prevenção, tratamento e resposta a incidentes cibernéticos;

VIII – articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação; e

IX – garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado e inviolabilidade da vida privada, da honra e da imagem das pessoas.

Art. 24. São objetivos da PSEC-PJ:

I – contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio de ações de segurança cibernética, observados os direitos e as garantias fundamentais;

II – fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética;

III – aprimorar continuamente o arcabouço normativo relacionado à segurança cibernética;

IV – fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança cibernética;

V – fortalecer a cultura de segurança cibernética no âmbito do Poder Judiciário;

VI – aprimorar o nível de maturidade em segurança cibernética no Poder Judiciário;

VII – orientar ações relacionadas:

a) à gestão em segurança da informação;

b) à segurança da informação das infraestruturas críticas;

c) ao tratamento das informações com restrições de acesso;

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

e) à prevenção, ao tratamento e à resposta a incidentes cibernéticos;

f) à gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos;

g) ao estabelecimento dos níveis de maturidade em segurança cibernética; e

h) ao estabelecimento de processo transparente de comunicação e respostas a incidentes entre o poder público e a sociedade.

Art. 25. São instrumentos da PSEC-PJ:

I – a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

II – o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ);

III – o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC-PJ);

IV – o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ).

§ 1º Os protocolos previstos neste artigo deverão ser revisados sempre que necessário, por ato do Presidente do CNJ.

§ 2º Além dos protocolos previstos nesta Resolução, serão aprovados por ato do Presidente do CNJ os Manuais de Referência para o gerenciamento, controle e padrões necessários ao aperfeiçoamento da segurança cibernética.

Art. 26. Todos os órgãos do Poder Judiciário, à exceção do STF, deverão adotar e seguir, além dos Manuais de Referência para o gerenciamento, controle e padrões necessários ao aperfeiçoamento da segurança cibernética, o PPINC-PJ, que deverá contemplar um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível; o PGCC-PJ, objetivando contribuir para a resiliência corporativa por meio de resposta, tão célere e eficiente quanto possível, a incidentes em que os ativos de

informação do Poder Judiciário tenham a sua integridade, confidencialidade ou disponibilidade comprometidos em larga escala ou por longo período; e o PIINC-PJ, com a finalidade de estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicar fatos penalmente relevantes aos órgãos de investigação e com atribuição para o início da persecução penal.

Parágrafo único. O PGCC-PJ complementa o PPINC-PJ e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar por tempo indeterminado.

Art. 27. Considerado o incidente como crise cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Incidentes e de Crises Cibernéticas.

Art. 28. Cada tribunal, com exceção do STF, deverá estabelecer em sua Política de Segurança da Informação ações para:

I – realizar a Gestão dos Ativos de Informação e da Política de Controle de Acesso;

II – criar controles para o tratamento de informações com restrição de acesso;

III – promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética;

IV – estabelecer requisitos mínimos de segurança cibernética nas contratações e nos acordos que envolvam a comunicação com outros órgãos;

V – utilizar os recursos de soluções de criptografia, ampliando o uso de assinatura eletrônica, conforme legislações específicas; e

VI – comunicar e articular as ações de segurança da informação com a alta administração do órgão.

CAPÍTULO VIII
DA GESTÃO DE USUÁRIOS

Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:

I – gerenciamento de identidades;

II – gerenciamento de acessos; e

III – gerenciamento de privilégios.

Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de *login* único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais.

CAPÍTULO IX
DA POLÍTICA DE CULTURA E EDUCAÇÃO EM SEGURANÇA CIBERNÉTICA

Art. 30. Fica instituída, no âmbito dos órgãos do Poder Judiciário, à exceção do STF, a Política de Cultura e Educação em Segurança Cibernética no âmbito do Poder

Judiciário (PCESC-PJ).

Parágrafo único. A PCESC-PJ será disciplinada por ato do Presidente do CNJ.

CAPÍTULO X
DO ORÇAMENTO

Art. 31. Para execução das ações estratégicas, os órgãos do Poder Judiciário, objeto desta norma, deverão destinar os recursos orçamentários necessários.

Parágrafo único. Os recursos orçamentários deverão ser discriminados em rubrica específica para possibilitar que a Governança Nacional em Segurança Cibernética possa avaliar, de forma clara, os investimentos no setor.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 32. Poderão ser instituídos planos de ações para detalhar a forma de aplicação da presente estratégia de segurança cibernética de acordo com a prioridade definida pelo CGSI-PJ.

Art. 33. Outros instrumentos complementares poderão ser elaborados e formalizados em normativos específicos do órgão desde que não contrariem as disposições estabelecidas nesta Resolução.

Art. 34. Ficam revogadas as Resoluções CNJ nº 360/2020; nº 361/2020 e nº 362/2020.

Art. 35. Ficam revogados os arts. 39 e 40 da Resolução CNJ nº 370/2021.

Art. 36. Esta Resolução entra em vigor na data de sua publicação.

Ministro LUIZ FUX

Fonte: Diário da Justiça [do] Conselho Nacional de Justiça, Brasília, DF, n. 149, p. 2-8, 10 jun. 2021.