Texto compilado a partir da redação dada pela Portaria SG n. 87/2021.

PORTARIA SECRETARIA-GERAL N. 47 DE 29 DE NOVEMBRO DE 2017

Institui a Política de Segurança da Informação do Conselho Nacional de Justiça.

O SECRETÁRIO-GERAL DO CONSELHO NACIONAL DE JUSTIÇA (CNJ), no uso de suas atribuições legais e regimentais,

CONSIDERANDO que o Conselho Nacional de Justiça recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;

CONSIDERANDO o número progressivo de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO a Portaria CNJ n. 112, de 11 de julho de 2013, que institui o Comitê de Gestor de Segurança da Informação (CGSI) do Conselho Nacional de Justiça;

CONSIDERANDO a Portaria CNJ n. 113, de 11 de julho de 2013, que institui o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) do Conselho Nacional de Justiça;

CONSIDERANDO a Portaria CNJ n. 35, de 12 de julho de 2013, que institui o Comitê de Gestão de Tecnologia da Informação e Comunicação (CGETIC) do Conselho Nacional de Justiça;

CONSIDERANDO os termos da Resolução CNJ n. 211, de 15 de dezembro de 2015, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e estabeleceu as diretrizes para sua governança, gestão e infraestrutura.

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Dos Princípios Básicos da PSI

Art. 1º Instituir a Política de Segurança da Informação (PSI) do Conselho Nacional de Justiça, que tem como princípios básicos:

I – a proteção do direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição Federal;

II – a proteção de informações relacionadas a assuntos que mereçam tratamento especial;

III – a capacitação dos segmentos das tecnologias sensíveis;

IV – a criação, desenvolvimento e manutenção de cultura relacionada à segurança da informação, alinhada as diretrizes nacionais de segurança da informação.

Seção II

Das Definições relativas à PSI

Art. 2º Para efeitos desta Política, ficam estabelecidos os seguintes conceitos:

I – ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, a integridade, a autenticidade e a disponibilidade da informação;

II – ativo de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III – autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;

IV – confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

V – disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;

VI – gestor de ativo de informação: são os titulares das unidades responsáveis pela gestão e operação dos ativos de informação;

VII – incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

VIII – informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

IX – integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

X – plano de continuidade de serviços essenciais: documentação dos procedimentos e informações necessárias para manter os ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo previamente definido, em casos de incidentes;

XI – plano de recuperação de serviços essenciais: documentação dos procedimentos e informações necessárias para que se operacionalize o retorno das atividades críticas à normalidade;

XII – público alvo: é o conjunto de usuários internos e externos atendidos pela Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais do CNJ (ETIR-CNJ);

XIII – risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XIV – segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XV – serviços essenciais: são aqueles que são imprescindíveis à atividade finalística deste Conselho;

XVI – unidade gestora de segurança da informação: é a unidade responsável pela gestão de segurança da informação no Conselho Nacional de Justiça;

XVII – usuário externo: qualquer pessoa física ou jurídica, não caracterizada como usuário interno, que tenha acesso a informações produzidas pelo Conselho Nacional de Justiça de forma autorizada;

XVIII – usuário interno: qualquer servidor, prestador de serviço terceirizado, estagiário ou qualquer outro colaborador que tenha acesso às informações produzidas pelo CNJ de forma autorizada; e

XIX – vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorado negativamente por uma ou mais ameaças.

Seção III

Dos Objetivos da PSI

Art. 3º São objetivos desta Política de Segurança da Informação:

I – dotar as unidades do Conselho Nacional de Justiça de instrumentos jurídicos, normativos e organizacionais que as capacitem a assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações produzidas e armazenadas;

II – estabelecer diretrizes e normas gerais para a efetiva implementação da segurança da informação;

III – subsidiar a promoção das ações necessárias à implementação e à manutenção dos processos de gestão de riscos, gestão de incidentes de segurança da informação, gestão da continuidade de serviços essenciais e gestão do uso dos recursos de Tecnologia da Informação e Comunicação; e

IV – promover o intercâmbio científico-tecnológico entre o Conselho Nacional de Justiça, os órgãos e entidades do Poder Judiciário e as instituições públicas e privadas sobre as atividades de segurança da informação.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Seção I

Da Classificação e Tratamento da Informação

Art. 4º A classificação e o tratamento da informação, realizados por meio de procedimento definido formalmente, abrange informações provenientes dos serviços essenciais de Tecnologia da Informação e Comunicação do Conselho Nacional de Justiça.

Parágrafo único. As informações deverão ser classificadas de forma a permitir tratamento diferenciado de acordo com seu grau de importância, criticidade, sensibilidade, e em conformidade com requisitos legais.

Art. 5º Os critérios gerais aplicáveis à Classificação e ao tratamento da informação serão definidos por normativo elaborado pelo Comitê Gestor de Segurança da Informação, com a participação de todas as unidades do Conselho Nacional de Justiça que produzem, recepcionam ou custodiam informações essenciais às atividades finalísticas, e submetido à apreciação da Presidência.

Seção II

Da Gestão de Riscos de Segurança da Informação

Art. 6º A gestão de riscos é realizada por meio de processo definido de maneira formal, contendo as fases de análise, avaliação e tratamento dos riscos.

Parágrafo único. O processo de gestão de riscos deverá, sempre que possível e necessário, ser apoiado por uma ferramenta computacional que contemple as atividades mencionadas no caput deste artigo.

Art. 7º Os gestores dos ativos de informação são os responsáveis pela execução das fases de análise, avaliação e tratamento dos riscos.

Parágrafo único. A unidade gestora de segurança da informação supervisionará os gestores de ativos de informação nas atividades mencionadas no caput deste artigo.

Art. 8º O escopo da gestão de riscos será definido anualmente pelo Departamento de Tecnologia da Informação e Comunicação, com a anuência do Comitê Gestor de Segurança da Informação, mantendo a correspondência com os serviços essenciais, preferencialmente.

Parágrafo único. Os critérios gerais aplicáveis para aceitação de riscos serão definidos anualmente pelo Comitê Gestor de Segurança da Informação, com a orientação técnica do Departamento de Tecnologia da Informação e Comunicação.

Art. 9º A unidade gestora de segurança da informação elaborará relatório anual de gestão riscos para o Comitê Gestor de Segurança da Informação, contendo as ações tomadas frente às ameaças e as recomendações utilizadas para tratar os riscos identificados.

Seção III

Da Gestão do Acesso e Uso dos Recursos de Tecnologia da Informação e Comunicação

Art. 10. A gestão de acesso e uso dos recursos de Tecnologia da Informação e Comunicação disponibilizados pelo Conselho Nacional de Justiça é regulado por normativo próprio.

Art. 11. Estão sujeitos à regulamentação de que trata o caput do art 10 os usuários internos e externos do Conselho Nacional de Justiça que, de maneira autorizada, tenham acesso aos recursos de Tecnologia da Informação e Comunicação prestados por este Conselho.

Parágrafo único. A utilização desses recursos está condicionada à aceitação desta Política por parte dos usuários mediante assinatura de termo de uso, preferencialmente em meio eletrônico.

Seção IV

Da Gestão e Controle de Ativos de Informação

Art. 12. A gestão e controle dos ativos de informação é realizada por meio de processo definido de maneira formal, contendo as fases de cadastro, atualização e exclusão.

Parágrafo único. O processo de gestão e controle dos ativos de informação deverá, sempre que possível e necessário, ser apoiado por ferramenta computacional que contemple as atividades mencionadas no caput deste artigo.

Art. 13. Os gestores dos ativos de informação são os responsáveis pela execução das fases de cadastro, atualização e exclusão.

Parágrafo único. A unidade gestora de segurança da informação do Conselho Nacional de Justiça supervisionará os gestores de ativos de informação nas atividades mencionadas no caput deste artigo.

Seção V

Da Gestão de Incidentes de Segurança da Informação

Art. 14. A gestão de incidentes de segurança da informação é realizada por meio de processo definido de maneira formal, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Art. 15. Fica instituída a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais do Conselho Nacional de Justiça (ETIR-CNJ), composta inicialmente por um servidor da Coordenadoria de Infraestrutura e Atendimento e um servidor da unidade responsável pela gestão de segurança da informação do Departamento de Tecnologia da Informação e Comunicação. (redação dada pela Portaria SG n. 87, de 20.9.2021).

Parágrafo único. A ETIR-CNJ poderá solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

Art. 16. A ETIR-CNJ tem autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão caso as recomendações não forem seguidas.

Parágrafo único. O Comitê Gestor de Segurança da Informação é o fórum para aprovar as ações decorrentes de um incidente ou ameaça de segurança que afetem a imagem institucional ou a confidencialidade das informações do Conselho Nacional de Justiça.

Art. 17. O funcionamento da ETIR-CNJ é regulado por documento formal de constituição, publicado no sítio eletrônico do Conselho Nacional de Justiça na Internet, devendo constar, no mínimo, os seguintes pontos: definição da missão, público alvo, modelo de implementação, canal de comunicação de incidentes de segurança e os serviços que serão prestados.

Seção VI

Da Gestão da Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação

Art. 18. A gestão da continuidade dos serviços essenciais de Tecnologia da Informação e Comunicação é realizada por meio de processo definido de maneira formal, contendo as fases de análise de impacto e definição das estratégias pelos Comitê

Gestor de Segurança da Informação e Comitê de Governança da Tecnologia da Informação e Comunicação do CNJ e, por fim, a elaboração de planos.

§ 1º Os planos mencionados no caput deste artigo são:

a) o de Continuidade de serviços essenciais de Tecnologia da Informação e Comunicação; e

b) o de Recuperação de serviços essenciais de Tecnologia da Informação e Comunicação.

§ 2º Os planos referidos no § 1º serão submetidos ao Comitê de Gestão de Tecnologia da Informação e Comunicação (CGETIC).

Art. 19. A definição dos serviços essenciais será feita pelo Comitê de Governança de Tecnologia da Informação e Comunicação, com apoio técnico do Departamento de Tecnologia da Informação e Comunicação.

Art. 20. A unidade gestora de segurança da informação do Conselho Nacional de Justiça é responsável por estabelecer e manter o processo formal da gestão de continuidade de serviços essenciais de Tecnologia da Informação e Comunicação.

Art. 21. Os gestores dos ativos de informação são os responsáveis pela elaboração dos procedimentos técnicos constantes nos Planos de Continuidade e de Recuperação de serviços essenciais de Tecnologia da Informação e Comunicação.

Art. 22. Os Planos de Continuidade e de Recuperação de serviços essenciais de Tecnologia da Informação e Comunicação, após aprovados, serão exercitados e testados anualmente e os resultados documentados de forma a garantir a sua efetividade.

Art. 23. Os Planos de Continuidade e de Recuperação de serviços essenciais de Tecnologia da Informação e Comunicação serão revisados nas seguintes situações:

I – no mínimo, uma vez por ano;

II – em função dos resultados dos testes realizados; e

III – após alguma mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes

CAPÍTULO III

DAS RESPONSABILIDADES

Seção I

Do Comitê Gestor de Segurança da Informação

Art. 24. Cabe ao Comitê Gestor de Segurança da Informação, assessorado pelo Departamento de Tecnologia da Informação, adotar as seguintes diretrizes:

I – propor normas e procedimentos internos relativos à segurança da informação, em conformidade com as legislações existentes sobre o tema;

II – promover cultura de segurança da informação no Conselho Nacional de Justiça e implementar programas contínuos destinados à conscientização e capacitação dos usuários interno;

III – propor recursos necessários às ações de segurança da informação;

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

V – estabelecer critérios de classificação dos dados e das informações, com vistas à garantia dos níveis de segurança desejados e à normatização do acesso e uso das informações;

VI – garantir que os objetivos propostos no art. 3º desta Política sejam alcançados.

Seção II

Do Departamento de Tecnologia da Informação e Comunicação

Art. 25. Cabe ao Departamento de Tecnologia da Informação e Comunicação implantar e gerenciar os controles relativos:

I – à gestão dos ativos de Tecnologia da Informação e Comunicação, principalmente os críticos e estratégicos, a fim de inventariar e identificar seus responsáveis;

II – à gestão da segurança das configurações da rede de comunicação de dados, para garantir a proteção das informações disponíveis na rede e a infraestrutura de suporte;

III – à gestão da segurança física dos ambientes computacionais, a fim de impedir e/ou repelir o acesso físico não autorizado e a ocorrência de danos e interferências nas instalações e informações digitais do órgão;

IV – à gestão das operações tecnológicas, a fim de garantir a operação segura dos recursos de processamento da informação;

V – à gestão das cópias e restauração de dados do CNJ, para manter a confidencialidade, a integridade e a disponibilidade das informações e dos recursos de processamento de informação;

VI – ao uso dos recursos tecnológicos e aos acessos às informações e serviços em rede do Conselho Nacional de Justiça, a fim de garantir o acesso somente aos usuários autorizados a operar as informações acessadas;

VII – ao gerenciamento de incidentes de segurança da informação, a fim de permitir o controle das fragilidades, vulnerabilidades e eventos que porventura

coloquem em risco a segurança das informações e serviços do Conselho Nacional de Justiça;

VIII – às modificações nos recursos de processamento da informação e sistemas do CNJ, considerando a criticidade dos sistemas e serviços essenciais.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 26. A Secretaria-Geral e a Diretoria-Geral, no âmbito de suas respectivas competências, são as unidades competentes para deliberar, em caráter definitivo, sobre as ações previstas no art. 24, seja por avocação ou por provocação.

Art. 27. A inobservância dos dispositivos constantes desta Política de Segurança da Informação pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 28. A Política de Segurança da Informação deverá ser revisada bianualmente ou quando necessário.

Art. 29. Esta Portaria entra em vigor na data de sua publicação.

Juiz **Júlio Ferreira de Andrade**