DIÁRIO DA JUSTIÇA

CONSELHO NACIONAL DE JUSTIÇA

Edição nº 205/2017 Brasília - DF, disponibilização quinta-feira, 7 de dezembro de 2017

SUMÁRIO

Presidência

Secretaria Geral

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

Seção I

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 pelos servidores da unidade responsável pela gestão de segurança da informação do Departamento de Tecnologia da Informação e Comunicação.

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**

INSTRUÇÃO NORMATIVA SG/PRESIDÊNCIA N. 2 DE 29 DE NOVEMBRO DE 2017

Dispõe sobre o provimento e a gestão de soluções de *software* no Conselho Nacional de Justiça.

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

CONSIDERANDO a necessidade de definir as responsabilidades das unidades envolvidas com o provimento e a gestão das soluções de *software* utilizadas no Conselho Nacional de Justiça;

CONSIDERANDO a necessidade de assegurar a participação dos usuários finais e dos gestores da informação na definição e na validação de requisitos e regras de negócio, assim como na homologação das soluções de *software*;

CONSIDERANDO a Resolução CNJ n. 211/2015, que dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e dá outras providências;

CONSIDERANDO a Portaria CNJ n. 85/2016, que instituiu o Plano Estratégico de Tecnologia da Informação e Comunicação do Conselho Nacional de Justiça (PETIC-CNJ) para o período de 2016-2020;

CONSIDERANDO os sistemas estratégicos e a prioridade de manutenção/sustentação de soluções constantes do Portfólio de Sistemas de Informação do Conselho Nacional de Justiça;

CONSIDERANDO a importância de estabelecer processos de trabalho, responsabilidades e práticas compatíveis com os modelos reconhecidos mundialmente, como a norma NBR ISO/IEC 38500:2009, o *ControlObjectives for InformationandRelated Technologies (Cobit)*, a *Information Technology Infrastructure Library (ITIL)* e a série de normas NBR ISO/IEC 20000:2008;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º O provimento e a gestão de soluções de *software* do Conselho Nacional de Justiça observarão o disposto nesta Instrução Normativa, que tem por objetivo contribuir para a eficiência, a eficácia e a efetividade na execução dos processos de trabalho que utilizam soluções de *software.*

Parágrafo único. As unidades envolvidas com o provimento e a gestão de soluções de *software* são solidariamente responsáveis pelo cumprimento harmônico das competências atribuídas nesta Instrução Normativa.

Art. 2º Para efeito do disposto nesta Instrução Normativa, entende-se por:

I - Acordo de Nível de Serviço: compromisso estabelecido entre a unidade provedora e a unidade gestora da solução de *software*, no qual se estabelecem níveis de serviço no ambiente de produção, considerando-se as necessidades das unidades orgânicas do Conselho Nacional de Justiça, o impacto, o custo e a capacidade de alocação de recursos para o provimento da solução, a exemplo de: horário de funcionamento, tempo máximo de resposta, quantidade mínima de transações a processar e nível mínimo de disponibilidade.

II - Ambiente de Produção: ambiente computacional para uso efetivo da solução de *software*, contendo a infraestrutura necessária ao adequado funcionamento da solução para os usuários.

III - Central de Serviços de Tecnologia da Informação e Comunicação (TIC): equipe responsável pelo atendimento centralizado dos usuários das soluções de *software* do Conselho Nacional de Justiça.

IV - Gestor da Informação: unidade orgânica que, no exercício de suas competências, produz informações ou obtém, de fonte externa ao Conselho Nacional de Justiça, informações de propriedade de pessoa física ou jurídica.

V - Homologação: conjunto de ações solicitadas pela unidade gestora que objetiva verificar a conformidade de uma solução de *software* às respectivas regras de negócio e requisitos coletados pela unidade provedora da solução.

VI - Módulo de Solução de *Software*: subconjunto de funcionalidades correlatas de uma solução de *software* agrupadas para fins de gestão.

VII - Partes Interessadas: indivíduos, unidades ou organizações que estejam diretamente envolvidos na gestão e na implementação da solução de *software* ou que, ainda que de forma indireta, possam influenciar ou ser afetados pela solução.

VIII - Portfólio de Soluções de Tecnologia da Informação e Comunicação: base de dados que mantém as seguintes informações relativas às soluções de software – sigla (se houver), nome do sistema, descrição do sistema estratégico, área gestora, área responsável TIC (provedora da solução), observação, endereço de produção e o resultado da priorização para identificação dos níveis de serviço acordados.

IX - Provimento de Solução de *Software*: conjunto de ações necessárias para implantar a solução de *software*, assegurar seu funcionamento e dar suporte adequado a seus usuários, podendo realizar-se nas modalidades desenvolvimento, aquisição, manutenção ou sustentação de *software.*

X - Regras de Negócio: regras inerentes ao processo de trabalho que determinam o comportamento de funcionalidades da solução de *software* e como as informações são processadas.

XI - Requisitos da Solução de *Software*: capacidades ou características que a solução de *software* deve apresentar ou condições que deve atender com vistas à realização de seu propósito.

XII - Roteiro de Atendimento: conjunto de instruções destinadas à Central de Serviços de TIC que orientam o atendimento de ocorrências e requisições e o esclarecimento de dúvidas relativas à solução de *software*.

XIII - Solução de *Software*: solução que automatiza processos de trabalho por meio do processamento sistemático de dados, tendo em vista a produção de resultados que atendam às necessidades das unidades orgânicas do Conselho Nacional de Justiça.

XIV - Solução Finalística de *Software*: destinada ao atendimento de necessidades finalísticas e estratégicas do Conselho Nacional de Justiça ou de outros Órgãos do Poder Judiciário, com impacto significativo nos resultados ou no funcionamento desses.

XV - Unidade Gestora da Solução de *Software*: responsável por definições relativas a processos de trabalho, regras de negócio e requisitos de solução de *software*, bem como por acordar os níveis de serviços com a unidade provedora da solução, nos termos desta Instrução Normativa.

XVI - Unidade Provedora da Solução de *Software*: unidade técnica responsável por coordenar os esforços de provimento de solução de *software* e as interações com a unidade gestora.

XVII - Unidade Superior de Governança (USG): unidade responsável por decisões que impactem no provimento, na gestão e na utilização das soluções de *software* nas unidades a ela subordinadas.

XVIII - Unidade de Serviços e Infraestrutura: unidade responsável por coordenar os esforços de provimento de serviços e infraestrutura de TIC.

§ 1º Para efeitos desta Instrução Normativa, a Coordenadoria de Gestão de Sistemas (COGS) e a Divisão de Gestão do Processo Judicial Eletrônico (DPJE), unidades vinculadas ao Departamento de Tecnologia da Informação e Comunicação (DTI), serão responsáveis pelo provimento de soluções de *software* do Conselho Nacional de Justiça.

§ 2º Será considerado Unidade Superior de Governança (USG) o Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) do Conselho Nacional de Justiça.

§ 3º A Coordenadoria de Atendimento e Infraestrutura (COAI), unidade vinculada ao DTI, será responsável pelo provimento dos recursos de TIC necessários ao adequado funcionamento das soluções de *software*.

CAPÍTULO II

DA CLASSIFICAÇÃO DAS SOLUÇÕES DE *SOFTWARE*

Art. 3º As soluções de *software* classificam-se nos seguintes tipos:

I - Solução Interna: sistema de informação desenvolvido internamente, recebido de outros órgãos ou entidades ou adquirido de terceiros pelo Conselho Nacional de Justiça, que será mantido pela unidade provedora responsável.

II - Solução Externa: sistema de informação desenvolvido e mantido por outra instituição, cujo acesso seja permitido a partir do ambiente computacional do Conselho Nacional de Justiça.

III - Solução Colaborativa: sistema de informação desenvolvido e mantido por uma ou mais instituições, cujo acesso seja permitido a partir do ambiente computacional do Conselho Nacional de Justiça ou demais órgãos.

IV - *Software* de Apoio: aplicativo ou utilitário adquirido ou utilizado pelo Conselho Nacional de Justiça.

V - Serviço Básico: serviços relativos à infraestrutura de comunicação, armazenamento, hospedagem e segurança de dados e informações, assim como outras soluções integradas de *software* e *hardware* presentes no ambiente computacional do Conselho Nacional de Justiça.

CAPÍTULO III

DOS REQUISITOS DAS SOLUÇÕES DE *SOFTWARE*

Art. 4º Consideram-se requisitos de uma Solução de *Software*:

I - Funcionalidade: conjunto de capacidades, ações e resultados que uma solução de *software* deve possuir, realizar ou produzir para atender às necessidades das unidades orgânicas do Conselho Nacional de Justiça e para assegurar níveis adequados de segurança da informação.

II - Usabilidade: conjunto de aspectos relativos à interação do usuário com a solução de *software*, consideradas a acessibilidade e a satisfação com a solução.

III - Confiabilidade: conjunto de atributos relacionados à frequência, gravidade e possibilidade de recuperação de falhas, bem como à exatidão dos resultados gerados pela solução de *software*.

IV - Desempenho: conjunto de atributos relativos à eficiência da solução de *software* em operação, tais como tempo de resposta e quantidade de recursos utilizados.

V - Suportabilidade: conjunto de aspectos relacionados à instalação, à configuração e à capacidade de adaptação, de manutenção/sustentação e de teste da solução.

VI - Integração: conjunto de aspectos relacionados ao compartilhamento de funcionalidades e de informações com outras soluções de *software* em utilização ou em desenvolvimento no Conselho Nacional de Justiça ou, ainda, com soluções de outros órgãos da administração pública.

VII - Segurança da Informação: conjunto de aspectos relacionados à confidencialidade, integridade e disponibilidade dos dados e informações gerados ou tratados pela solução e de outros aspectos gerais de segurança, a exemplo de critérios para definição de perfis de acesso a funcionalidades, rastreamento de ações realizadas, verificação de autenticidade e garantia de não repúdio, além.

CAPÍTULO IV

DAS DEMANDAS PARA PROVIMENTO

DE SOLUÇÃO DE *SOFTWARE*

Art. 5º As demandas para provimento e manutenção/sustentação de soluções de *software* com impacto significativo sobre o PETIC-CNJ e, consequentemente, no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), serão encaminhadas por meio de processo administrativo e deverão ser submetidas à análise prévia do DTI, por meio do Documento de Oficialização de Demanda (DOD).

§ 1º A solicitação a que se refere o *caput* deste artigo compete à unidade demandante da solução de *software*, com apoio do DTI, e constitui condição indispensável à apreciação da demanda.

§ 2º Compete ao DTI apreciar a solicitação a que se refere o *caput* deste artigo e, com base nas informações presentes no DOD, elaborar documento de Análise de Viabilidade da Demanda (AVD).

§ 3º O DTI, auxiliado pela unidade demandante, poderá realizar estudos complementares que se fizerem necessários, como estimativas de custos, análise de riscos e levantamento de alternativas no mercado, tendo em vista a necessidade de embasar decisão acerca da forma de provimento de solução de *software* mais vantajosa para o Conselho Nacional de Justiça.

§ 4º O início das atividades de provimento da solução de *software* ocorrerá somente após a aprovação formal da Análise de Viabilidade da Demanda pela Unidade Superior de Governança.

§ 5º A aprovação formal referida no § 4º deste artigo deverá observar o alinhamento da nova demanda com o Planejamento Estratégico Institucional e o de TIC.

§ 6º Na hipótese de a análise de viabilidade indicar ser mais vantajoso o provimento da solução de *software* mediante contratação, o processo de provimento a ser seguido observará o disposto em norma específica do Conselho Nacional de Justiça que disponha sobre as contratações de Solução de TIC no Poder Judiciário e em outras normas que disponham sobre licitações e contratos.

§ 7º Na hipótese de a análise de viabilidade indicar ser mais vantajoso o provimento da solução de *software* mediante desenvolvimento interno ou colaborativo, o processo de provimento a ser seguido observará o disposto no Processo de Desenvolvimento e Sustentação de Sistemas (PDS) do DTI.

§ 8º Os documentos necessários ao planejamento, execução, homologação, entrega e até exclusão da solução de *software* do portfólio do Conselho Nacional de Justiça e demais registros relevantes deverão ser incluídos em processo administrativo, visando garantir a preservação do histórico da demanda.

§ 9º As soluções de *software* a serem mantidas e os novos sistemas de informação de procedimentos judiciais deverão também atender aos requisitos elencados na ENTIC-JUD e em outras normas específicas publicadas pelo Conselho Nacional de Justiça.

CAPÍTULO V

DAS COMPETÊNCIAS DA UNIDADE SUPERIOR DE GOVERNANÇA

Art. 6º Compete à Unidade Superior de Governança, para efeito do disposto nesta Instrução Normativa, em relação ao provimento de soluções de *software* nas unidades a ela subordinadas:

I - avaliar as demandas de que trata o art. 5º desta Instrução Normativa;

II - decidir quanto à natureza, à prioridade e à modalidade de provimento da solução de *software*;

III - designar a unidade gestora e aprovar, quando couber, as atualizações nos planos pertinentes;

IV - decidir quanto à alteração de unidade gestora e sobre a descontinuidade de solução de *software*; e

V - autorizar o início das atividades de provimento da solução de *software* em qualquer de suas modalidades.

§ 1º Em caso de impossibilidade de atendimento simultâneo das demandas de provimento de solução de *software* apresentadas pelas Unidades de Governança Superior, compete ao Secretário-Geral, em nome da Presidência do Conselho Nacional de Justiça, estabelecer o ordenamento das prioridades, considerando a estratégia, as diretrizes de gestão, a urgência e os recursos disponíveis.

§ 2º A designação de unidade gestora para cada uma das soluções de *software* constantes do Portfólio de Soluções do Conselho Nacional de Justiça constitui condição indispensável ao início das atividades de provimento e recairá, preferencialmente, sobre unidade que, em função da sua competência institucional, detenha maior conhecimento e autonomia de decisão sobre as informações e os processos de trabalho abrangidos pela solução de *software*.

§ 3º A critério da Unidade Superior de Governança, poderá ser designada unidade gestora para solução de *software,* especialmente quando o provimento tiver impacto relevante sobre o Plano Estratégico do Conselho Nacional de Justiça ou quando a solução servir a processos de trabalho que envolvam diferentes unidades organizacionais.

CAPÍTULO VI

DAS COMPETÊNCIAS DA UNIDADE GESTORA DA SOLUÇÃO DE *SOFTWARE*

Art. 7º Compete à unidade gestora da solução de *software*, independentemente da natureza da solução e da modalidade de provimento utilizada:

I - identificar as necessidades institucionais a serem atendidas pela solução de *software;*

II - mapear ou modelar os processos de trabalho a serem informatizados, buscando, caso necessário, o auxílio do Departamento de Gestão Estratégica, para maximizar os benefícios proporcionados pela utilização da solução;

III - autorizar, em conjunto com a unidade provedora da solução de *software*, o início de atividades de provimento da solução de *software;*

IV - solicitar, fundamentadamente, a suspensão, o cancelamento ou a alteração de atividade de provimento previamente autorizada;

V - definir, mediante consulta a representantes de usuários, gestores da informação e outras partes interessadas, os requisitos e as regras de negócio da solução de *software*, bem como acordar com a unidade provedora os níveis de serviço da solução, visando ampliar os benefícios ao Conselho Nacional de Justiça e promover a integração com as demais soluções;

VI - propiciar a participação de representantes de usuários e dos gestores da informação no Conselho Nacional de Justiça, para auxiliar na definição ou validação de regras de negócio, requisitos e níveis de serviço e na homologação da solução de *software*;

VII - apoiar a unidade provedora da solução de *software* na realização dos estudos complementares de que trata o § 3º do art. 5º desta Instrução Normativa;

VIII - solicitar à Secretaria de Gestão de Pessoas, durante o projeto de desenvolvimento ou contratação da solução de *software*, o planejamento das ações de treinamento para uso da solução;

IX - propor, quando necessário, a criação ou alteração de normativos para regulamentar os processos de trabalho apoiados pela solução de *software*;

X - elaborar e manter atualizados roteiros de atendimento da solução de *software*, com apoio da unidade provedora;

XI - homologar a solução de *software* e, se for o caso, fundamentar, dentro dos prazos acordados com a unidade provedora, a não homologação.

XII - definir, em conjunto com a unidade provedora, estratégia de implantação da solução, considerando a necessidade de capacitação dos usuários e, quando for o caso, a realização de implantação em regime de projeto piloto;

XIII - apoiar ou exercer, em conjunto com a unidade provedora, a fiscalização dos contratos, acordos de cooperação e outros instrumentos congêneres relativos à solução de *software*;

XIV - elaborar, disponibilizar para consulta pelos usuários e manter atualizados, no Portal do Conselho Nacional de Justiça e/ou Intranet, manuais e roteiros de utilização, tutoriais e outras informações necessárias à correta utilização da solução de *software* e à compreensão dos processos de trabalho associados;

XV - propor à Secretaria de Gestão de Pessoas a realização de evento de capacitação voltado ao desenvolvimento de competências, quando forem identificadas dificuldades na utilização da solução de *software*;

XVI - participar do planejamento e da execução de ações de desenvolvimento de competências para utilização da solução;

XVII - acompanhar e avaliar a utilização da solução de *software* e, se necessário, adotar as medidas de sua competência ou solicitar providências para que a confidencialidade, a integridade e a disponibilidade da informação sejam preservadas, para que os benefícios esperados sejam alcançados e para que os acordos de nível de serviço sejam cumpridos;

XVIII - preparar e divulgar informes e dar orientações referentes a procedimentos de utilização da solução, sem prejuízo da atuação da Central de Serviços de TIC;

XIX - receber e analisar solicitações de mudanças ou informações relativas a regras de negócio e requisitos da solução de *software*, bem como adotar as providências de sua competência e comunicá-las aos solicitantes;

XX - propor à unidade provedora prioridades de atendimento de demandas relativas à solução de *software*, observadas as estratégias institucionais, os benefícios esperados e o custo estimado;

XXI - definir, ouvidos os gestores da informação, os requisitos de segurança para a solução, relacionados com a obtenção, tratamento, transmissão, uso, armazenamento e descarte das informações recebidas, produzidas ou tratadas pela solução de *software*;

XXII - definir e revisar periodicamente, ouvidos os gestores da informação, os privilégios, perfis e direitos de acesso de usuários às funcionalidades e às informações disponibilizadas pela solução de *software*, bem como as regras de concessão e revogação;

XXIII - avaliar a necessidade de serem implementadas, na solução de *software*, funcionalidades que permitam aos usuários e aos gestores da informação classificar, em conformidade com as normas institucionais pertinentes, os elementos de informação que produzirem ao utilizar a solução;

XXIV - manifestar-se quanto à conveniência e oportunidade de atendimento a solicitações de órgãos e entidades para cessão dos códigos-fonte da solução de *software* desenvolvida pelo Conselho Nacional de Justiça;

XXV - reavaliar, periodicamente, os benefícios, a necessidade e a efetividade da solução de *software* e informar à unidade provedora sobre razões que possam ensejar a descontinuidade da solução, para fins de manifestação dessa unidade técnica;

XXVI - coordenar, em conjunto com o DTI, negociações com os órgãos e entidades envolvidos, para modelar proposta de acesso e uso de solução de *software* externa pelo Conselho Nacional de Justiça, mediante celebração de instrumento específico; e

XXVII - autorizar, em conjunto com o DTI, a implantação inicial e posteriores mudanças da solução de *software* em ambiente de produção ou manifestar-se sobre os motivos da não autorização, dentro dos prazos acordados com a unidade provedora.

§ 1º O não cumprimento do prazo de homologação acordado com a unidade provedora poderá ensejar à unidade demandante a responsabilização prevista em contrato firmado com empresa fornecedora de solução de TIC, inclusive, se o atraso injustificado der causa à necessidade de liberação de pagamentos sem a devida homologação da solução de *software*.

§ 2º O titular da unidade gestora de solução de *software* deverá designar formalmente servidores com perfil adequado e em quantidade suficiente para exercer as competências previstas nesta Instrução Normativa, sem prejuízo do exercício de outras atribuições.

§ 3º A designação de que trata o parágrafo 2º deste artigo deverá ser comunicada ao DTI, para registro na base de informações de que trata o art. 12 desta Instrução Normativa, e poderá, a critério do titular da unidade gestora, ser efetuada com fundamento em competências específicas.

§ 4º Quando da definição de regras de negócio ou requisitos que afetem outras soluções de *software*, a unidade gestora deverá, em conjunto com a unidade provedora da solução, promover as negociações necessárias com as partes interessadas.

§ 5º O DTI disciplinará papéis e responsabilidades específicos em caso de desenvolvimento e manutenção/sustentação de soluções de *software* com uso de recursos de terceiros e, em se tratando do Processo Judicial Eletrônico (PJe), as citadas deliberações ficarão a cargo do Comitê Gestor Nacional do PJe.

§ 6º O benefício da integração a ser alcançado mediante o disposto no inciso V deste artigo objetiva evitar a redundância de informações entre as soluções de *software* contratadas ou desenvolvidas pelo Conselho Nacional de Justiça.

CAPÍTULO VII

DAS COMPETÊNCIAS DO DEPARTAMENTO DE

TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 8º Compete ao DTI, para efeito do disposto nesta Instrução Normativa:

I - analisar e, quando necessário, encaminhar à Unidade Superior de Governança as demandas de que trata o art. 5º desta Instrução Normativa, acompanhadas da motivação e de parecer com proposta de designação da unidade gestora da solução, além de proposta de prioridade, modalidade e abordagem de provimento; e

II - analisar e, quando necessário, encaminhar à Unidade Superior de Governança as sugestões de alteração de unidade gestora, bem como as solicitações de descontinuidade de solução de *software* de natureza corporativa, acompanhadas de parecer que fundamente as referidas sugestões ou solicitações.

CAPÍTULO VIII

DAS COMPETÊNCIAS DA COORDENADORIA DE GESTÃO

DE SISTEMAS (COGS) E DA DIVISÃO DE GESTÃO DO

PROCESSO JUDICIAL ELETRÔNICO (DPJE)

Art. 9º Compete à COGS e à DPJE, como unidades do DTI e provedoras de soluções de *software*, além de suas competências institucionais:

I - definir processos, métodos, técnicas, ferramentas e padrões aplicáveis ao provimento de soluções de *software*, disponíveis no processo de desenvolvimento/sustentação de sistemas do Conselho Nacional de Justiça;

II - negociar, junto à unidade gestora e demais partes interessadas, escopo e prazos do projeto de desenvolvimento, manutenção/sustentação ou contratação de solução de *software*, respeitadas as premissas e restrições estabelecidas nos planos de TIC do Conselho Nacional de Justiça;

III - definir, em conjunto com a unidade gestora, a estratégia de implantação e de sustentação durante a fase de estabilização da solução de *software*;

IV - avaliar as regras de negócio, os requisitos e os níveis de serviço definidos pela unidade gestora da solução de *software* e apontar possíveis inconsistências ou incompatibilidades, para promover a integração das soluções de *software*, a padronização da arquitetura tecnológica e a maximização dos benefícios para o CNJ;

V - desenvolver a solução de *software* ou planejar e solicitar sua aquisição, de acordo com as regras de negócio e os requisitos especificados pela unidade gestora;

VI - manter a unidade gestora e demais partes interessadas informadas sobre o andamento de demandas e projetos relativos à solução de *software;*

VII - fiscalizar, tecnicamente, com o apoio ou em conjunto com as respectivas unidades gestoras, contratos, acordos de cooperação ou instrumentos congêneres relativos a soluções de *software*;

VIII - realizar os testes necessários para assegurar o correto funcionamento e a aderência da solução de *software* às regras de negócio, aos requisitos e aos acordos de níveis de serviço, principalmente a realização dos testes de segurança para os sistemas estratégicos do Conselho Nacional de Justiça;

IX - manter a unidade gestora e demais partes interessadas informadas sobre paradas programadas e incidentes relacionados à solução de *software* nos ambientes de homologação, de treinamento e de produção;

X - apoiar, no âmbito de sua área de atuação, as unidades gestoras no planejamento e execução de ações de desenvolvimento de competências para utilização de soluções de *software*;

XI - apoiar as unidades gestoras na formulação de propostas de prioridades de atendimento de demandas relativas a cada solução de *software*, consolidar as propostas apresentadas pelas unidades e encaminhá-las às instâncias competentes para subsidiar o planejamento das ações de TIC;

XII - solicitar, quando necessário, a atuação das unidades envolvidas na gestão e no provimento de soluções de *software*, no que se refere ao desempenho das competências previstas nesta Instrução Normativa;

XIII - realizar, mediante autorização da Unidade Superior de Governança, as modificações necessárias para a cessão dos códigos-fonte das soluções de *softwares* do Conselho Nacional de Justiça a outros órgãos e entidades;

XIV - realizar em conjunto com a unidade demandante da solução de *software*, quando couber, os estudos complementares de que trata o § 3º do art. 5º desta Instrução Normativa; e

XV - manifestar-se quanto aos aspectos técnicos e custos envolvidos no atendimento a solicitação de cessão de código-fonte de solução de *software* desenvolvida pelo Conselho Nacional de Justiça;

Parágrafo único. Os níveis de serviço acordados para a solução de *software* pela unidade provedora e gestora deverão ser fundamentados em acordos operacionais firmados entre as demais unidades técnicas do DTI, considerada a real capacidade de atendimento dessas unidades.

CAPÍTULO IX

DAS COMPETÊNCIAS DA COORDENADORIA

DE ATENDIMENTO E INFRAESTRUTURA (COAI)

Art. 10. Compete à COAI, como unidade do DTI e provedora de serviços e infraestrutura de TIC, além de suas competências institucionais:

I - prover ambiente computacional adequado para desenvolvimento, teste, homologação, treinamento e uso das soluções de *software;*

II - definir, em conjunto com a unidade provedora, a estratégia de implantação e de sustentação durante a fase de estabilização da solução de *software*, relativamente aos aspectos de infraestrutura;

III - assegurar o funcionamento da solução de *software* de acordo com os níveis de serviço acordados;

IV - apoiar a unidade gestora da solução de *software* na elaboração de roteiros de atendimentos; e

V - decidir, em situação de emergência, sobre a interrupção de funcionamento de solução de *software* que esteja degradando o desempenho ou afetando o funcionamento das demais soluções.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 11. As responsabilidades das unidades gestora e provedora e das demais partes envolvidas na cessão dos códigos-fonte, a outros órgãos e entidades, de soluções de *software* desenvolvidas pelo Conselho Nacional de Justiça serão estabelecidas observando-se, para cada caso concreto, limites e condições indicados no respectivo instrumento de cessão.

Art. 12. As unidades gestoras das soluções de *software* serão registradas em base de informação própria para manutenção desse registro, o qual será parte integrante do portfólio de sistemas de informação a ser disponibilizado para consulta pelo público interno, no Portal e/ou Intranet do Conselho Nacional de Justiça.

Art. 13. Esta Instrução Normativa entra em vigor na data de sua publicação.

Juiz **Júlio Ferreira de Andrade**