ABMES

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 09/10/2023 | Edição: 193 | Seção: 1 | Página: 26
Órgão: Ministério da Educação/Fundo Nacional de Desenvolvimento da Educação

PORTARIA Nº 647, DE 5 DE OUTUBRO DE 2023

Institui a Política de Governança Digital do Fundo Nacional de Desenvolvimento da Educação - FNDE e dá outras providências.

A PRESIDENTE DO FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO - FNDE, no uso de suas atribuições legais, com base no art. 3º da Lei n. 5.537, de 21 de novembro de 1968, no inciso II, do art. 17, Anexo I, do Decreto 11.196, de 13 de setembro de 2022, e no inciso II do art. 190 da Portaria/FNDE n. 742, de 06 de dezembro de 2022, resolve:

Art. 1°. Instituir, na forma do ANEXO ÚNICO a esta Portaria, a POLÍTICA DE GOVERNANÇA DIGITAL do Fundo Nacional de Desenvolvimento da Educação - FNDE, constituída pelo conjunto de princípios, diretrizes, objetivos, políticas, práticas, estruturas e competências organizacionais com a finalidade de habilitar e extrair valor institucional do uso eficiente, controlado e justificado dos recursos de Tecnologia da Informação e Comunicação, tanto nas atividades finalísticas quanto naquelas de suporte interno, no âmbito da Autarquia, buscando balancear a autonomia regimental com os objetivos de controle desejados para a organização.

Parágrafo Único. A Política de Governança Digital do FNDE poderá ser revista a qualquer tempo, mediante deliberação do Comitê de Governança Digital, a fim de assegurar seu alinhamento às prioridades e estratégias institucionais e às mudanças na legislação vigente.

Art. 2°. Fica revogada a Portaria nº 571, de 25 de setembro de 2018.

Art. 3°. Esta Portaria entra em vigor, após 5 dias da sua publicação.

FERNANDA MARA DE OLIVEIRA MACEDO CARNEIRO PACOBAHYBA

ANEXO ÚNICO

POLÍTICA DE GOVERNANÇA DIGITAL DO FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

Art.1°. A POLÍTICA DE GOVERNANÇA DIGITAL do FNDE aborda o conjunto de princípios, diretrizes, objetivos, políticas, práticas, estruturas e competências organizacionais para habilitar e extrair valor institucional do uso eficiente, controlado e justificado dos recursos de Tecnologia da Informação e Comunicação, tanto nas atividades finalísticas quanto naquelas de suporte interno, no âmbito da Autarquia, buscando balancear a autonomia regimental e o nível dos controles de gestão desejados pela organização.

Parágrafo único. O modelo de governança digital abordado nesta política oferece uma matriz capaz de se adaptar aos diferentes contextos da Autarquia, desde situações em que haja necessidade de maiores níveis de controle até os cenários com maior abertura à experimentação, no conceito metodológico de Governança Adaptativa.

CAPÍTULO II - DOS CONCEITOS E DEFINIÇÕES

Art. 2°. Para fins de aplicação nesta POLÍTICA, foram considerados os seguintes conceitos:

I - Alta administração: agentes públicos formalmente designados que atuam como dirigentes máximos na Autarquia;

II - Comitê de Governança Digital (CGD): estrutura colegiada, de caráter estratégico e deliberativo, para deliberar sobre princípios, diretrizes, políticas e planos relacionados à Governança Digital, Tecnologia da Informação e Comunicação, Segurança da Informação e das Comunicações, Segurança Cibernética, Governança de Dados, Dados Abertos e outros temas correlacionados;

II - Subcomitê Executivo de Tecnologia da Informação e Comunicação (SeTIC): colegiado técnico de caráter executivo e consultivo, subordinado ao Comitê de Governança Digital, cuja finalidade é desenvolver, aprovar e monitorar serviços, padrões, processos e metodologias da área de Tecnologia da Informação e Comunicação - além de avaliar a viabilidade técnica e econômica, aprovar, acompanhar tecnicamente os projetos de TIC e assessorar o Comitê de Governança Digital nos assuntos de sua competência;

III - Subcomitê de Governança e Proteção de Dados (SeGPD): colegiado técnico multidisciplinar de caráter executivo e consultivo, subordinado ao Comitê de Governança Digital, cuja finalidade é propor, monitorar e avaliar o conjunto de políticas, processos, procedimentos e controles para garantir a gestão adequada e eficaz dos dados no âmbito do FNDE, além de assessorar o Comitê de Governança Digital nos assuntos de sua competência;

IV - Subcomitê de Segurança da Informação (SeSIC): colegiado técnico multidisciplinar de caráter executivo e consultivo, subordinado ao Comitê de Governança Digital, cuja finalidade é propor, monitorar e avaliar o conjunto de políticas, processos, procedimentos e controles relacionados à segurança da informação, segurança cibernética, privacidade e proteção de dados no âmbito do FNDE, além de assessorar o Comitê de Governança Digital nos assuntos de sua competência;

V - Computação em Nuvem (cloud computing): modelo de fornecimento de recursos de computação como serviço mantido e gerenciado por provedores de serviços em nuvem e acessíveis, sob demanda, por meio de uma rede (geralmente a internet), que possam incluir processamento, armazenamento, bancos de dados, rede, software, análise e inteligência baseada em dados;

VI - Comunicação Unificada: processo que unifica os dispositivos tecnológicos de comunicação de uma organização em uma única plataforma, possibilitando o acesso padronizado e permitindo que os usuários possam compartilhar e acessar dados e colaborar entre si em tempo real;

VII - Custo Total de Propriedade (Total Cost of Ownership - TCO): métrica utilizada para identificar todos os custos que cercam a oferta de um produto ou serviço, considerando seus custos diretos, indiretos e não aparentes;

VIII - Dados abertos: dados que podem ser livremente utilizados, reutilizados e redistribuídos por qualquer pessoa, sujeitos, no máximo, à exigência de atribuição à fonte original e ao compartilhamento pelas mesmas licenças no qual as informações foram apresentadas, condição geralmente satisfeita pela publicação desses dados em formato aberto e sob uma licença aberta;

IX - DevOps: abordagem colaborativa e integrada para o desenvolvimento de software (Dev) e operações de TI (Ops) que visa quebrar as barreiras entre as equipes de desenvolvimento e operações, promovendo a comunicação, automação e compartilhamento de responsabilidades com ênfase à entrega contínua e rápida de software de alta qualidade, por meio da automação de processos e colaboração efetiva entre equipes - melhorando a eficiência, a confiabilidade e a agilidade dos projetos de software;

X - DevSecOps: prática de incorporar a segurança cibernética (Sec) no desenvolvimento de software (Dev) e nas operações de TI (Ops), visando integrar a segurança em todos os estágios do ciclo de vida do desenvolvimento de software, desde o planejamento e design até a implantação e sustentação de modo a torná-la componente fundamental em todo o processo;

XI - Diretoria de Tecnologia e Inovação (DIRTI): órgão seccional da estrutura organizacional responsável por planejar, coordenar e executar as atividades inerentes à gestão de tecnologia de informação e comunicação e da segurança da informação e comunicações no âmbito do FNDE;

XII - Estratégia de Governança Digital (EGD): documento que define os objetivos estratégicos, as metas, os indicadores e as iniciativas da Política de Governança Digital do Poder Executivo Federal;

XIII - Governança Adaptativa: modelo de governança que reconhece a natureza dinâmica dos ambientes e busca criar estruturas de governança que se ajustem e evoluam conforme necessário, equilibrando a necessidade de controle e conformidade com a flexibilidade exigida para enfrentar os desafios em constante mudança;

XIV - Governança de TIC: sistema pelo qual o uso atual e futuro de TIC é dirigido e controlado, mediante avaliação e direcionamento, para atender às necessidades prioritárias e estratégicas da organização e monitorar sua efetividade por meio de planos, incluída a estratégia e as políticas de uso de TIC no âmbito da organização;

XV - Gestão de TIC: é o conjunto de ações relacionadas ao planejamento, desenvolvimento, execução e monitoramento das atividades de TIC, em linha com a direção definida pela função de governança, a fim de atingir os objetivos institucionais;

XVI - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC): instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TIC que visa

a atender as necessidades tecnológicas e de informação de um órgão ou entidade para determinado período;

XVII - Plano de Transformação Digital (PTD): é o instrumento de planejamento de um determinado setor de governo que visa refletir todos os esforços de transformação digital de cada órgão ou entidade da administração pertencente aquele setor;

XVIII - Tecnologia da Informação e Comunicação (TIC): ativo estratégico que suporta processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e usar informações; e

XIX - Transformação Digital: fenômeno que incorpora o uso da tecnologia digital à solução de problemas tradicionais e criação de produtos e serviços digitais. Abrange mudanças procedurais em diversos âmbitos e modifica o paradigma da utilização da tecnologia.

CAPÍTULO III - DOS PRINCÍPIOS E OBJETIVOS

SEÇÃO I - DOS PRINCÍPIOS

Art.3°. São princípios orientadores da Política de Governança Digital do FNDE:

I - entregar valor para a organização, os usuários e a sociedade: todas as soluções e serviços digitais devem gerar valor real para as partes interessadas, representadas pelos agentes internos, mercado privado e sociedade na sua totalidade;

II - criar um ambiente de inovação: a inovação deve ser reconhecida, valorizada e estimulada em todos os níveis como um agente catalisador de mudanças que tem em vista encontrar novas formas de impactar os serviços públicos e a vida dos cidadãos e da sociedade, através da experimentação, substituição de estruturas inadequadas, eliminação do medo de errar e do uso de novas tecnologias - incluindo a discussão sobre uso de Inteligência Artificial;

III - promover a colaboração e a cooperação: a definição, o desenvolvimento e o fomento de iniciativas digitais e de Tecnologia da Informação devem priorizar o diálogo colaborativo com as áreas internas, entidades vinculadas, órgãos da Administração Pública, mercado e sociedade - promovendo, sempre que possível, o compartilhamento de infraestruturas, soluções, serviços e dados visando eliminar a duplicação de esforços e reduzir custos;

IV - simplificar processos: produtos e serviços de Tecnologia da Informação devem buscar reduzir a complexidade, a fragmentação e a duplicação das informações através da digitalização e/ou da otimização de processos de ponta-a-ponta através, por exemplo, da hiperautomação inteligente - com foco na eficiência e eficácia;

V - fomentar o modelo de Governo como Plataforma: as soluções digitais devem considerar, sempre que viável, a arquitetura de Governo com uma plataforma aberta, a partir da qual possam ser geradas oportunidades para uso de informações públicas visando o fomento à inovação e o desenvolvimento científico, social e econômico do país;

VI - garantir a segurança e a privacidade de dados e informações: produtos e serviços digitais devem garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações, além de proteger o sigilo e a privacidade dos dados, na forma da lei;

VII - promover a integridade e a transparência: ações de TIC devem ser balizadas pela integridade, ao passo onde os projetos, os custos, os riscos e os resultados deverão ser medidos e reportados à alta administração e à sociedade por meio de canais de comunicação

adequados, proporcionando a devida transparência na aplicação dos recursos públicos e o amplo acesso na divulgação de informações relevantes;

VIII - prestar contas e definir responsabilidades: os papéis e responsabilidades envolvidos nos processos de tomadas de decisão em TIC, deverão ser definidos, compreendidos e aceitos de maneira clara e sem ambiguidade, para assegurar a adequada prestação de contas das ações, bem como a responsabilização pelos atos praticados - flexibilização e descentralização serão consideradas sempre que possível neste processo;

IX - promover a confiança e a adaptabilidade: direitos decisórios em processos de governança digital devem ser definidos, compreendidos e aceitos de maneira clara e sem ambiguidade, na perspectiva de implementação de práticas e processos flexíveis que se adaptem segundo as necessidades de gestão e controle - sendo imprescindível promover um ambiente de transparência, confiança e adaptabilidade;

X - estar em conformidade: a governança digital deve buscar gerar e promover uma cultura organizacional de ética, transparência e eficiência, de modo que todas as ações estejam alinhadas com as estratégias corporativas e as obrigações regulamentares, legislativas, legais e contratuais aplicáveis.

SEÇÃO II - DOS OBJETIVOS

Art.4°. São objetivos gerais da Política de Governança Digital do FNDE:

I - estabelecer um modelo de governança adequado às necessidades corporativas da Autarquia;

II - prover alinhamento contínuo das práticas de governança digital às estratégias, planos e políticas institucionais e de TIC do FNDE;

III - possibilitar a elevação gradativa e contínua da maturidade das práticas e processos de governança de TIC com relação aos resultados, à transparência, ao controle e à otimização de recursos e capacidades;

IV - garantir a adequação em relação a leis e normas vigentes no se refere a processos de transparência e acesso a informações, respeitados os procedimentos de classificação de informações e proteção de dados;

V - alavancar a entrega de resultados, qualificar a relação organizacional entre a área de TI e as demais áreas da Autarquia - contribuindo com os processos de governança corporativa; e

VI - contribuir com o alcance dos objetivos estabelecidos na Estratégia de Governança Digital (EGD), do Governo Federal.

CAPÍTULO IV - DAS ESTRUTURAS ORGANIZACIONAIS

Art.5°. A estrutura central de apoio à Governança Digital no FNDE é o Comitê de Governança Digital, colegiado deliberativo estratégico responsável por dirigir o alinhamento das ações e dos investimentos em TIC para o alcance dos objetivos institucionais, priorizando-as adequadamente - além de definir metas e avaliar resultados.

§1°. A existência e operacionalização de um Comitê de Governança Digital para deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de Tecnologia da Informação e Comunicação atende ao disposto no Decreto n.º 10.332, de 28 de abril de 2020.

§2°. De modo a reduzir a complexidade institucional, caso haja expressa necessidade, poderão ser criados subcomitês temáticos vinculados ao Comitê de Governança

Digital para apoiar a governança e a gestão de TIC no FNDE, considerando suas diversas disciplinas, observadas as competências regimentais.

CAPÍTULO V - DAS DIRETRIZES

SEÇÃO I - DAS DIRETRIZES GERAIS

Art. 6°. São diretrizes gerais da Política de Governança Digital do FNDE:

I - as ações de TIC devem ser dirigidas e controladas mediante a utilização de instrumentos de avaliação, direção e monitoramento visando identificar oportunidades e iniciativas que otimizem seus usos e viabilizem a estratégia digital do FNDE;

II - a interoperabilidade e o uso de padrões tecnológicos e de segurança da informação nas soluções digitais devem ser continuamente aprimorados com foco em capacidades de Governança de Dados, transparência pública e segurança cibernética;

III - o compartilhamento e integração de dados, processos, sistemas, serviços e infraestruturas de TIC devem ser consideradas prioritariamente como estratégias para promover a ampliação e a melhoria contínua dos serviços digitais do FNDE, em estrita harmonia com a legislação vigente; e

IV - o Plano Diretor de Tecnologia da Informação e Comunicação deve ser o principal instrumento de planejamento setorial de TIC, visando a unificação e a manutenção do alinhamento estratégico dos instrumentos de planejamento institucional.

SEÇÃO II - DAS DIRETRIZES ESPECÍFICAS

Art. 7°. As diretrizes específicas aplicam-se aos seguintes domínios temáticos:

I - governança, planejamento e gestão de TIC;

II - governança de dados;

III - governança de aquisições e gestão de fornecedores;

IV - gestão de talentos em TIC;

V - gestão da inovação em TIC;

VI - gestão do orçamento e das finanças de TIC;

VII - gestão de demandas e da capacidade;

VIII - gestão de projetos de TIC;

IX - gestão de padrões e de arquiteturas de TIC

X - gestão de serviços de TIC;

XI - gestão de infraestrutura de TIC;

XII - gestão de sistemas e aplicações;

XIII - gestão de segurança da informação, privacidade e proteção de dados;

XIV - gestão da continuidade do negócio; e

XV - gestão de riscos de TIC, integridade, controles internos e conformidade.

SUBSEÇÃO I - DA GOVERNANÇA, DO PLANEJAMENTO E DA GESTÃO DE TIC

Art. 8°. A governança, o planejamento e a gestão dos recursos de Tecnologia da Informação e Comunicação devem ser realizados de maneira sistemática e contínua, para proporcionar a tomada de decisão com base em evidências - corrigindo desvios, identificando oportunidades de melhoria e promovendo o aprendizado organizacional, observadas as seguintes diretrizes específicas:

I - o planejamento setorial de TIC deve ser entendido como um desdobramento natural e necessário do planejamento estratégico institucional, que visa a definir diretrizes e ações transversais de TIC alinhadas aos objetivos estratégicos da Autarquia;

II - o planejamento setorial de TIC deve zelar pelo contínuo alinhamento estratégico por meio do diálogo e da colaboração permanente entre as estruturas organizacionais, viabilizando a ampla participação das diversas áreas na elaboração das estratégias, planos, ações e projetos;

III - a área de TIC deve construir e manter uma compreensão holística e multidisciplinar da organização e de seus processos de trabalho, para identificar oportunidades que possam ser alavancadas pela aplicação de recursos digitais;

IV - o planejamento de TIC deve visar a construção de estratégias que contemplem objetivos, metas e indicadores de curto, médio e longo prazos - bem como prioridades e iniciativas alinhadas às estratégias organizacionais e de Governo, com acompanhamento contínuo;

V - devem ser implementadas ações e iniciativas que visem o fortalecimento do modelo de governança em rede, da cultura ágil, das práticas de integração e aumento contínuo do nível de maturidade dos processos de gestão, potencializando o uso de recursos digitais como instrumento de inovação, automação inteligente, integração e incremento da produtividade por meio da transformação digital de produtos, serviços e processos;

VI - devem ser implementadas e mantidas ações técnicas e gerenciais com o intuito de garantir a disponibilidade, a confiabilidade e a integridade dos dados, informações, recursos e ambientes de TIC, direcionando investimentos adequados em soluções de computação em nuvem e segurança cibernética, sempre que viável; e

VII - devem ser implementadas e mantidas ações técnicas e gerenciais que garantam a implementação da Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) de modo a proporcionar a evolução contínua da maturidade em governança de dados corporativos e o fornecimento de inteligência contínua para suportar as políticas públicas educacionais.

Art. 9°. Para implementar as diretrizes específicas de governança, gestão e planejamento de TIC, bem como contribuir para o alcance dos objetivos estratégicos institucionais, na forma do art. 3º do Decreto n.° 10.332, de 28 de abril de 2020, deverão ser elaborados e mantidos vigentes e atualizados os seguintes instrumentos, aprovados pelo Comitê de Governança Digital:

I - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

II - Plano de Transformação Digital (PTD); e

III - Plano de Dados Abertos (PDA).

§1°. O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), deve ser entendido como o instrumento de planejamento setorial único - harmonizado e integrado ao Planejamento Estratégico Institucional e capaz de fornecer direcionamento estratégico e tático para todas as iniciativas, ações e projetos de TIC da Autarquia.

§2°. O Plano de Transformação Digital (PTD) poderá ser elaborado e coordenado pelo órgão setorial do SISP ao qual o FNDE está vinculado (Ministério da Educação - MEC), contendo as ações e compromissos específicos da Autarquia.

§3°. Periodicamente, a instituição deve avaliar os processos de governança, gestão e planejamento de TIC quanto ao grau de cumprimento das suas diretrizes pelos atores envolvidos em sua execução, bem como avaliar o desempenho dos próprios processos com base em sua eficiência, eficácia e efetividade.

Art. 10. A comunicação sobre os resultados da governança, da gestão e do uso de TIC é de responsabilidade da Diretoria de Tecnologia e Inovação - DIRTI e tem por objetivo garantir a transparência ativa e a publicidade dos resultados nos meios de comunicação oficiais do FNDE e nos canais públicos, conforme o caso, considerando, no mínimo, o seguinte:

I - manter planos estratégicos, táticos e operacionais vigentes e disponíveis para todas as partes interessadas;

II - manter disponíveis e atualizadas informações sobre o alcance dos objetivos planejados, viabilizando o acompanhamento contínuo das ações, dos programas e dos projetos;

III - publicar, na forma da Lei, estudos técnicos preliminares e documentos relacionados a editais de contratações de TIC, assim como os contratos e seus respectivos aditivos;

IV - manter disponíveis e atualizados o Catálogo de Serviços de TIC, o Catálogo de Sistemas e Aplicações e o Catálogo de Dados;

V - manter disponíveis e atualizadas as informações sobre orçamento e execução orçamentária de TIC, ao longo do exercício;

VI - manter repositório com documentos de auditorias, avaliações e respostas oficiais aos questionários sobre a maturidade em governança e gestão de TIC conduzidos pelos órgãos de controle e/ou pelo órgão central do SISP, bem como os respectivos relatórios de resultados dessas avaliações;

VII - manter repositório das atas de reuniões do Comitê de Governança Digital, incluindo suas deliberações.

§1°. As comunicações devem atender, no que for cabível, às disposições contidas na Lei de Acesso à Informação (LAI), na Lei Geral de Proteção de Dados (LGPD) e na Política de Dados Abertos (PDA) do Poder Executivo Federal quando da divulgação das informações sobre a gestão e o uso de TIC.

§2° Todas as comunicações devem garantir a adequação entre o meio, o formato e o respectivo público-alvo, com uso de linguagem simples e sempre conforme as políticas e normas corporativas de comunicação.

SUBSEÇÃO II - DA GOVERNANÇA DE DADOS

Art. 11. A governança de dados deve observar as seguintes diretrizes específicas:

I - deve haver adequada definição de papéis e responsabilidades relacionados à governança de dados, com necessário envolvimento de todas as partes interessadas;

II - dados devem ser tratados como ativo institucional, considerando todo o seu ciclo de vida, objetivando criar um ambiente de coordenação e confiança;

III - um processo de gestão da qualidade de dados deve ser implementado e gerenciado, considerando, inclusive, métricas adequadas;

IV - devem ser implementados e gerenciados processos e políticas de segurança e privacidade, com objetivo de garantir a preservação dos atributos fundamentais dos dados corporativos.

V - as atividades de governança e gestão de dados devem ser continuamente monitoradas e aprimoradas, objetivando garantir o compliance regulatório, jurídico e setorial; e

§1°. As práticas corporativas de governança de dados deverão considerar o contexto no qual a Autarquia está inserida, buscando promover a integração e a transparência de dados entre as diretorias, comitês, conselhos e colegiados que compõem a estrutura do FNDE e entre esses e os demais entes governamentais, subnacionais e societais.

§2°. As práticas de transparência ativa devem assegurar o acesso aos dados e informações públicas existentes, em formato aberto, permitida sua livre utilização, consumo e cruzamento - com foco na elaboração e manutenção do Plano de Dados Abertos do FNDE.

§3°. Deve ser instituído um Subcomitê de Governança de Dados, como estrutura subordinada ao Comitê de Governança Digital, para tratar dos assuntos específicos relacionados ao conjunto de políticas, processos, procedimentos e controles que visem garantir a gestão adequada e eficaz dos dados no âmbito do FNDE.

§4°. Os processos de governança de dados devem ser periodicamente avaliados com relação ao grau de implementação de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

SUBSEÇÃO III - DA GOVERNANÇA DE AQUISIÇÕES E GESTÃO DE FORNECEDORES

Art. 12. A governança de aquisições e a gestão de fornecedores de TIC devem observar as seguintes diretrizes específicas:

I - promoção da ética nas contratações públicas, incluindo construção de normativos internos que objetivem a garantia da impessoalidade e do tratamento adequado de eventuais conflitos de interesse entre agentes públicos e privados;

II - integração e alinhamento das contratações de TIC ao Planejamento Estratégico Institucional - PEI, ao Plano Diretor de TIC - PDTIC e ao Plano de Contratações Anual - PCA, devendo ser considerada a alocação orçamentária necessária para a realização das iniciativas planejadas e para o custeio dos contratos vigentes;

III - contratações de TIC deverão ser precedidas de planejamento, que conterá, no mínimo, a devida fundamentação da necessidade e a vinculação aos resultados pretendidos, baseadas em análises adequadas e suficientes, de modo a permitir a tomada de decisão com transparência e equilíbrio entre os benefícios, as oportunidades, os custos e os riscos envolvidos;

IV - sempre que técnica e economicamente viável, o planejamento de contratações deverá considerar a aquisição de soluções completas, com a previsão de itens relacionados à implantação, treinamento, suporte, operação e demais componentes necessários ao alcance dos objetivos definidos;

V - a remuneração de fornecedores deverá, sempre que aplicável, basear-se em resultados e entregas passíveis de verificação - incluindo fixação e avaliação de níveis mínimos de serviço e avaliação de desempenho dos fornecedores; e

VI - durante o processo de planejamento de contratações, quando couber, deverão ser incluídas cláusulas de preservação dos direitos de propriedade intelectual do FNDE sobre códigos-fonte, documentos e outros componentes de aplicações desenvolvidas especificamente para a Autarquia, com recursos próprios ou de terceiros.

Parágrafo único. Devem ser instituídos mecanismos para desenvolver a capacidade dos gestores e dos colaboradores em processos de aquisição e gestão de

fornecedores, incluindo alocação de pessoal com perfil adequado, sucessão de pessoal e capacitação contínua.

Art. 13. A gestão e o relacionamento com fornecedores devem observar, ainda, o seguinte:

I - o relacionamento com fornecedores, atuais ou potenciais, deverá ser norteado pela transparência e pela impessoalidade, tendo como objetivo promover a ética nas relações públicas e evitar situações de eventual conflito de interesses, nos termos da lei e das normas aplicáveis;

II - a realização de Provas de Conceito - PoC com soluções de mercado, fora do âmbito de licitações, deve se dar preferencialmente diretamente com os seus respectivos fabricantes, sendo que, em qualquer situação, o procedimento deve ser objeto de formalização com indicação clara do escopo, das partes envolvidas, das condições de realização e das responsabilidades pela manutenção das condições de proteção de dados e informações;

III - em consagração ao princípio da isonomia, não deve ser admitida a ocorrência de registro de oportunidade em nenhum segmento ou tipo de fornecedor, seja para fabricante ou revendedor.

SUBSEÇÃO IV - DA GESTÃO DE TALENTOS EM TIC

Art. 14. A gestão de talentos em TIC deve observar as seguintes diretrizes específicas:

I - incentivo à promoção de ações de desenvolvimento profissional e valorização das pessoas;

II - recrutamento e seleção de profissionais qualificados para todas as posições técnicas e gerenciais;

III - treinamento e desenvolvimento contínuo das pessoas, com foco no desenvolvimento de capacidades profissionais e interpessoais; e

IV - desenvolvimento e manutenção de um ambiente propício para o crescimento pessoal e a valorização profissional.

Art. 15. Os cargos de gestão de TIC do FNDE deverão ser ocupados, preferencialmente, por servidores públicos efetivos, empregados públicos ou militares, sendo que os processos de gerenciamento de talentos em TIC deverão, sempre que viável, observar o seguinte:

I - a seleção de talentos deverá ocorrer considerando a melhor adequação entre o perfil profissional e as atribuições das funções e/ou cargos da unidade de TIC;

II - as ações de treinamento e qualificação devem tem por objetivo promover o desenvolvimento contínuo de competências técnicas e gerenciais, conforme o perfil do cargo e/ou função;

III - a retenção de talentos deve buscar promover a valorização do quadro próprio, com ações de reconhecimento e merecimento, observados o grau de capacidade técnica e a correspondência das atribuições com o perfil profissional de cada indivíduo;

IV - os espaços de trabalho devem propiciar condições ambientais e técnicas adequadas ao exercício das atividades laborais e ao convívio entre as pessoas; e

V - os formatos alternativos de trabalho (trabalho remoto e/ou trabalho híbrido) devem ser considerados meios de alavancar a produtividade e a satisfação das pessoas, sem prejuízo ao cumprimento das normas institucionais sobre o tema.

SEÇÃO V - DA GESTÃO DA INOVAÇÃO EM TIC

Art. 16. A gestão e promoção das ações e iniciativas de inovação em TIC devem observar as seguintes diretrizes específicas:

I - estímulo à criatividade, empreendedorismo e busca por soluções inovadoras para incentivar e alavancar o uso de TICs como instrumento de incremento de capacidade, qualidade e produtividade - de forma orientada ao cidadão-usuário;

II - colaboração e troca de conhecimentos como métodos para desenvolvimento de um ambiente propício à inovação, promovendo mudança cultural e implementando os mecanismos necessários para capturar e registrar sugestões e ideias de projetos de inovação enviados por colaboradores internos e pelo público externo, a partir de critérios pré-estabelecidos;

III - aplicação de métodos e ferramentas para gerenciar o ciclo de vida do processo de inovação de modo a viabilizar a descoberta e a aplicação de novas tecnologias, ainda que em caráter experimental, considerando sempre o contexto e a viabilidade econômico-financeira, visando acelerar a disrupção digital;

IV - fomentar tanto as inovações tecnológicas baseadas em alta tecnologia como aquelas baseadas em simplicidade e baixo custo - considerando seu potencial de aplicabilidade e valor agregado;

V - incentivar a utilização dos instrumentos de fomentos contidos na Lei n.° 10.973, de 2 de dezembro de 2004 (Lei de Incentivo à Inovação), no Decreto n.° 10.534, de 28 de outubro de 2020 (Política Nacional de Inovação) e na Lei Complementar n.° 182, de 1.º de junho de 2021 (Marco Legal das Startups).

SUBSEÇÃO VI - DA GESTÃO DO ORÇAMENTO E DAS FINANÇAS DE TIC

Art. 17. Observadas as competências regimentais pertinentes, o gerenciamento orçamentário e financeiro deve observar as seguintes diretrizes específicas:

I - elaboração de um orçamento realista e alinhado com os objetivos organizacionais, considerando o adequado controle de custos, maximização do retorno sobre investimentos e otimização dos recursos financeiros;

II - o desenvolvimento e/ou aquisição de bens e/ou serviços de TIC deverá conter a estimativa do seu Custo Total de Propriedade (Total Cost of Ownership - TCO), considerando todo o ciclo de vida das soluções e seus impactos diretos e indiretos;

III - todas as despesas de TIC devem ser objeto de planejamento e, quando aplicável, submissão às instâncias de governança superior - conforme os limites definidos nos normativos internos e/ou externos - na forma da lei e das normas aplicáveis; e

IV - todos os elementos de despesa relativos aos bens e serviços de TIC deverão ser devidamente padronizados e estar em consonância com as diretrizes constantes no Manual Técnico de Orçamento - MTO e nos catálogos oficiais de materiais e de serviços.

§1°. Todos os gestores de contratos de TIC deverão ser envolvidos no processo de planejamento e monitoramento do ciclo orçamentário, sendo responsáveis por observar os limites e as disponibilidades financeiras e orçamentárias dos contratos sob sua gestão;

§2°. Todas as contratações de TIC, exceto nas situações legalmente previstas, devem ser precedidas de certificação da disponibilidade orçamentária para sua efetivação, assim como da elaboração do respectivo cronograma físico-financeiro de execução;

§3°. Todas as autorizações de fornecimento de bens e/ou serviços contratados devem ser precedidas de verificação da existência de saldo de empenho, ou de, no mínimo, certificação da disponibilidade orçamentária para fazer face à despesa, na forma da Lei.

SUBSEÇÃO VII - DA GESTÃO DE DEMANDAS E DA CAPACIDADE EM TIC

Art. 18. Todas as demandas e necessidades relacionadas a bens e/ou serviços de TIC devem ser sistematicamente registradas em um canal de entrada único (inventário) para serem devidamente entendidas, avaliadas, planejadas e priorizadas com objetivo de garantir o adequado dimensionamento e otimização da capacidade dos recursos de TIC, considerando as seguintes diretrizes específicas:

§1°. O inventário de demandas e necessidades deve ser entendido como um insumo essencial para o planejamento setorial de TIC e deve ser elaborado a partir da visão do demandante, considerando os objetivos e requisitos de negócio a serem atendidos.

§2°. Considerando o caráter finito dos recursos, todas as demandas devem sofrer processo de avaliação e priorização, objetivando garantir o alinhamento das prioridades organizacionais e seu balanceamento com a capacidade da área de TIC.

§3°. Investimentos em expansão e/ou criação de programas e políticas públicas devem ser acompanhados de investimentos proporcionais na expansão da capacidade dos recursos de TIC, de modo a garantir a adequada sustentabilidade de sua operacionalização.

Art. 19. Deverá ser executado um processo de gerenciamento da capacidade e desempenho objetivando garantir que os serviços e infraestruturas de TIC atendam aos requisitos relacionados à evolução das demandas institucionais e à manutenção e evolução do desempenho atual e futuro, considerando, no mínimo, o seguinte:

I - Deve ser desenvolvido e mantido um Plano de Capacidade envolvendo todos os recursos necessários para entregar os serviços de TIC a curto, médio e longo prazos - de forma aderente à evolução dos requisitos e necessidades do negócio.

II - Antes da entrada em produção de um novo serviço, produto ou sistema de TIC deve ser elaborado um Plano de Capacidade para adequado dimensionamento e alocação dos recursos de TIC necessários à sua operacionalização.

III - Nenhum novo serviço, produto ou sistema de TIC deve ser colocado em produção antes de cumpridas as seguintes etapas, no mínimo:

a) homologação pelo gestor de negócio;

b) aprovação técnica pela Diretoria de Tecnologia da Informação, incluindo elaboração e aprovação do Plano de Capacidade e provisionamento dos recursos de TIC adequados;

c) classificação quanto ao nível de criticidade; e

d) definição e implementação dos fluxos de suporte técnico e negocial, considerando a classificação de criticidade.

SUBSEÇÃO VIII - DA GESTÃO DE PROJETOS DE TIC

Art. 20. A gestão de projetos de TIC deve ter por objetivo assegurar que os projetos sejam adequadamente aprovados, planejados, executados e revisados com vistas à

ótima realização dos benefícios e a redução dos riscos, considerando as seguintes diretrizes específicas:

I - deve ser executado um processo de gestão de projetos de TIC, preferencialmente, como parte integrante de um processo institucional de gestão de projetos, cumprindo, no mínimo, as etapas de planejamento, execução, monitoramento e controle;

II - o escopo, os custos, o uso de recursos e o cumprimento de prazos devem ser gerenciados durante a execução de todos os projetos de TIC;

III - todos os projetos de TIC de alta materialidade ou alta relevância devem ser submetidos a um processo de gestão de riscos - incluindo o acompanhamento pelo Comitê de Governança Digital;

IV - todos os projetos de TIC deverão estar devidamente alinhados com as estratégias, planos e prioridades institucionais, contribuindo para o cumprimento da missão e o alcance das metas da organização;

V - o balanceamento do portfólio de projetos deverá utilizar critérios relacionados ao alinhamento com a estratégia organizacional, os retornos de curto, médio e longo prazos, os tipos de benefícios esperados, o grau de riscos e o impacto para a imagem institucional;

VI - o desempenho dos projetos e programas de TIC, incluindo seus indicadores, deverá ser reportado periódica e preferencialmente de forma ativa, a todas as partes interessadas envolvidas;

§1°. O processo de gestão de projetos deve ser periodicamente avaliado com relação ao grau de cumprimento de suas práticas, bem como avaliação de suas práticas quanto ao seu grau de eficiência, eficácia e efetividade - de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

§2°. Deve ser disponibilizado pela DIRTI painel gerencial destinado à alta administração para acompanhamento dos projetos de TIC, como foco naqueles classificados como prioritários e/ou estratégicos;

§3°. Os riscos de projetos devem ser mapeados, avaliados e monitorados tanto como parte do processo de gestão de projetos como no contexto do processo de gestão de riscos de TIC.

SUBSEÇÃO IX - DA GESTÃO DE PADRÕES E DE ARQUITETURAS DE TIC

Art. 21. As atividades, processos e arquiteturas de TIC devem ser referenciadas em padrões técnicos devidamente aprovados, documentados e comunicados, observadas as seguintes diretrizes específicas:

I - o modelo padronizado de arquitetura de TIC deverá ser composto por arquitetura de negócio, arquitetura da informação, arquitetura de aplicações e arquitetura de tecnologia;

II - devem ser estabelecidos e observados processos adequados para prospecção tecnológica e definição dos padrões técnicos e das arquiteturas de TIC, com o apoio do Comitê de Governança Digital e do Subcomitê Executivo de Tecnologia da Informação e Comunicação;

III - o modelo de arquitetura deve ser gerenciado e revisado periodicamente para assegurar o seu alinhamento ao cenário tecnológico e aos objetivos estratégicos institucionais;

IV - sempre que possível e tecnicamente viável deverão ser utilizados padrões de arquitetura com baixo acoplamento, priorizando-se modelos abertos, componíveis,

modulares, reutilizáveis, interoperáveis e facilmente escaláveis em detrimento dos padrões de arquitetura monolíticos, pouco flexíveis e de difícil manutenção;

V - no que couber, o modelo de arquitetura deve considerar os padrões de interoperabilidade e de governo eletrônico, definidos e mantidos pelos órgãos governantes superiores;

§1°. Os padrões e arquiteturas corporativas devem ser observados por toda a organização, ainda que nos projetos executados com terceiros utilizando recursos próprios das áreas.

§2°. Os processos de gestão de padrões e de arquiteturas de TIC devem ser periodicamente avaliados com relação ao grau de cumprimento de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade, de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

SUBSEÇÃO X - DA GESTÃO DE SERVIÇOS DE TIC

Art. 22. A gestão de serviços de TIC deve contemplar, no mínimo, todo o conjunto de processos cujo objetivo é assegurar que o provimento desses serviços seja feito de modo alinhado às necessidades corporativas, com qualidade adequada e otimização de custos e riscos, considerando as seguintes diretrizes específicas:

I - a prestação de serviços corporativos de TIC deverá ser realizada de forma centralizada pela Diretoria de Tecnologia e Inovação - prioritariamente por meio de uma Central de Serviços unificada;

II - os serviços devem ser relacionados e formalizados em um Catálogo de Serviços, cujo objetivo é disponibilizar aos usuários dos serviços e ao pessoal de suporte de forma tempestiva, atualizada e acessível o rol completo dos serviços de TIC disponíveis e das informações relevantes a eles associadas, como pontos de contato e horários de utilização e os Acordos de Níveis de Serviço (ANS) estabelecidos;

III - deve ser executado um processo de gestão de níveis de serviço com objetivo de definir, acordar, documentar, monitorar, reportar e analisar criticamente os serviços de TIC prestados, de modo a garantir que a sua entrega seja alcançável, gerenciada e alinhada com os requisitos de clientes e as necessidades do negócio;

IV - o desempenho dos serviços de TIC deve ser periodicamente avaliado para verificar o grau de aderência aos níveis de serviço, bem como avaliar o desempenho dos próprios processos (eficiência, eficácia e efetividade) com vistas à realização de ajustes, aperfeiçoamentos e melhoria contínua;

V - deve ser definido, mantido e executado um processo adequado de gestão de incidentes visando gerir o ciclo de vida de todos os incidentes e, para cada incidente, restabelecer o serviço de TIC aos usuários no menor prazo e com o menor impacto possível;

VI - deve ser definido, mantido e executado um processo adequado de gestão de mudanças, com objetivo de permitir que mudanças necessárias sejam feitas com a mínima interrupção dos serviços e mínimo impacto nos níveis de serviço estabelecidos;

VII - deve ser definido, mantido e executado um processo adequado de gestão de configuração e de ativos de serviço para manter informações relevantes sobre a configuração de ativos de TIC necessários à entrega dos serviços, incluindo os relacionamentos entre eles, durante todo seu ciclo de vida; e

§1°. Os processos de gestão de serviços de TIC devem ser periodicamente avaliados com relação ao grau de cumprimento de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

§2°. Os riscos operacionais relacionados aos serviços de TIC - referentes a possíveis impactos resultantes do baixo desempenho e/ou da indisponibilidade destes - devem ser identificados, avaliados e monitorados tanto como parte do processo de gestão de serviços como no âmbito do processo de gestão de riscos de TIC.

SUBSEÇÃO XI - DA GESTÃO DA INFRAESTRUTURA DE TIC

Art. 23. O gerenciamento da infraestrutura de TIC deve observar as seguintes diretrizes específicas:

I - sempre que técnica e economicamente viável, deve ser priorizada a adoção de recursos de computação em nuvem (cloud computing), seja nuvem pública ou privada, nas modalidades de Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) ou Software como Serviço (SaaS), com objetivo de otimizar o desempenho, reduzir a complexidade tecnológica, promover a orquestração entre ambientes e ampliar a capacidade, a gerenciabilidade, a escalabilidade e a elasticidade dos ambientes;

II - práticas de integração entre desenvolvimento, segurança e operações (DevOps e DevSecOps) deverão ser viabilizadas através da implementação de ferramentas e arquiteturas adequadas, como foco na otimização da capacidade de gerenciamento automatizado, repetível e seguro, conforme critérios de qualidade e disponibilidade, tanto para recursos físicos quanto virtuais ou em nuvem, gerando fluxos de trabalho propícios às práticas de integração contínua (CI) e entrega contínua (CD);

III - a rede de comunicação de dados e voz deve ser padronizada para toda a Autarquia, com convergência de tecnologias de voz sobre IP (VoIP) e comunicações unificadas (UC);

IV - infraestruturas críticas devem ser mapeadas e devidamente protegidas, incluindo soluções de contingência e de recuperação de desastres; e

V - os ativos de TIC devem inventariados, identificados e continuamente monitorados como parte do processo de gerenciamento de ativos.

Parágrafo único. Os processos de gestão de infraestrutura de TIC devem ser periodicamente avaliados com relação ao grau de implementação de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

SUBSEÇÃO XII - DA GESTÃO DE SISTEMAS E APLICAÇÕES

Art. 24. O FNDE deve possuir e executar um processo de software, assim entendido como o processo de trabalho usado pela organização na produção e na gestão do ciclo de vida de sistemas e aplicações - abrangendo as atividades realizadas desde a demanda, o provimento (desenvolvimento ou aquisição), a operação, a sustentação até a eventual desativação.

I - o processo de software deve considerar, no mínimo, as seguintes fases essenciais:

a) descoberta: identificação, compreensão e análise do problema, necessidade e/ou oportunidade de geração de valor;

b) desenho: definição dos objetivos do projeto, elaboração do escopo, priorização, definição e planejamento do Mínimo Produto Viável (MVP);

c) construção: desenvolvimento iterativo e incremental do produto, de acordo com os requisitos definidos e priorizados - incluindo a validação técnica e negocial (testes) das entregas para garantir que atendem aos requisitos e não contenham erros;

d) implantação: implementação da entrega em ambiente de produção;

e) entrega: entrega do produto e/ou do incremento ao cliente, considerando a validação do valor gerado; e

f) manutenção: manter o software atualizado e resolver quaisquer problemas que possam surgir.

II - o processo ágil de software deverá ser caracterizado por:

a) iteratividade: O processo é dividido em iterações curtas, geralmente de duas a quatro semanas. Isso permite que a equipe entregue software em funcionamento de forma rápida e frequente.

b) incrementalidade: O software é desenvolvido de forma incremental, ou seja, a cada iteração, uma nova funcionalidade é adicionada ao software. Isso permite que a equipe entregue software de alta qualidade de forma gradual.

c) participação do cliente: O cliente é envolvido no processo de desenvolvimento desde o início. Isso permite que o cliente dê feedback sobre o software em desenvolvimento e garante que o software atenda às suas necessidades.

III - o processo de software deve tratar, ainda, dos seguintes aspectos:

a) gestão da documentação;

b) gestão da configuração;

c) gestão da qualidade;

d) gestão da segurança;

e) gestão da disponibilidade; e

d) gestão do portfólio (ciclo de vida).

IV - sempre que tecnicamente viável, todos os sistemas e aplicações do FNDE devem possuir funcionalidade de gestão unificada de usuários (Single-Sign-On) e serem integrados ao Login Único do Governo Federal (Acesso Gov.br);

V - todos os sistemas e aplicações corporativas do FNDE devem possuir um gestor negocial formalmente designado e com atribuições claramente fixadas e compreendidas - com foco no gerenciamento do produto do ponto de vista do negócio; e

VI - os sistemas e aplicações de software destinadas ao uso corporativo pelo FNDE devem sofrer processo de classificação segundo a criticidade, considerando os aspectos como impacto para o negócio e a continuidade de serviços públicos essenciais, com objetivo de definir processos e níveis mínimos de serviço adequados a cada conjunto de soluções.

Parágrafo único. O processo de classificação de criticidade de sistemas e aplicações deve ser submetido à aprovação e acompanhamento pelo Comitê de Governança Digital.

Art. 25. O provimento de sistemas e aplicações de software compreende as seguintes modalidades:

I - desenvolvimento: construção de soluções, com recursos próprios e/ou de terceiros, para atender as necessidades corporativas das áreas-meio e/ou das áreas-fim;

II - aquisição: adoção, por meio de processo de contratação, de soluções prontas ou customizáveis;

III - evolução ou adaptação: melhoria de qualidade, incorporação de novas funcionalidades, mudança nas regras de negócio ou adaptação a novas tecnologias;

IV - sustentação: alteração de solução existente a partir de intervenções corretivas, análise e solução de incidentes e requisições de serviço relacionadas às soluções que não impliquem em mudanças de regras de negócio ou alterações estruturais de suas funcionalidades.

V - internalização: incorporação de soluções de software desenvolvidas externamente, quer de forma específica para atendimento das necessidades da Autarquia, cedidas por outros entes públicos ou privados, ou, ainda, de soluções de código aberto (open source), por quaisquer meios ou instrumentos legais admissíveis;

§1°. Independentemente da modalidade adotada, a abordagem gerencial, segundo a responsabilidade das unidades envolvidas, deve considerar as seguintes alternativas:

a) gestão centralizada: quando o desenvolvimento, a aquisição, a manutenção ou a internalização da solução forem realizados de forma direta e centralizada pela Diretoria de Tecnologia e Inovação;

b) gestão descentralizada: quando o desenvolvimento, a aquisição, a manutenção ou a internalização da solução forem realizados diretamente por outras unidades internas, sob gestão técnica da Diretoria de Tecnologia e Inovação; e

c) gestão compartilhada: quando o desenvolvimento, a aquisição, a manutenção ou a internalização da solução forem realizados com compartilhamento de responsabilidades entre a Diretoria de Tecnologia e Inovação e outras unidades internas.

§2°. A aplicação de quaisquer das modalidades e abordagens de provimento de soluções de software para uso corporativo do FNDE, incluindo as soluções de caráter departamental, se sujeita à prévia análise e manifestação técnica da Diretoria de Tecnologia e Inovação.

Art. 26. O desenvolvimento de soluções e produtos de software pelo FNDE deverá observar, ainda, as seguintes diretrizes específicas:

I - o desenvolvimento de sistemas e aplicações de software deve ter foco na otimização dos processos de trabalho, na capacidade de integração entre soluções e na reutilização de dados e componentes;

II - durante o processo de concepção e especificação de soluções de software devem ser considerados tanto os requisitos funcionais quanto os requisitos não funcionais relevantes, principalmente aqueles relacionados à segurança da informação, integração, disponibilidade, desempenho e usabilidade;

III - o contexto de utilização e os domínios funcionais das aplicações devem ser respeitados de modo que suas regras de negócio e funcionalidades sejam consistentes com seu propósito (finalidade), objetivando a evitar redundâncias funcionais, proliferação de soluções altamente pontuais, perda de integridade de dados e elevação dos custos de desenvolvimento e manutenção;

IV - os padrões técnicos e arquiteturais mantidos pela Diretoria de Tecnologia e Inovação devem ser obedecidos de modo a garantir a manutenibilidade e a capacidade de interoperabilidade entre os sistemas corporativos;

V - direitos de propriedade intelectual devem cobrir códigos-fonte, documentos e outros elementos integrantes de soluções desenvolvidas especificamente para a instituição, com recursos próprios ou de terceiros, devendo o FNDE possuir a guarda e a gestão desses itens;

VI - modelos de testes adequados devem ser utilizados para garantir a aderência das soluções às regras de negócio e aos requisitos especificados, como premissa para entrada em produção, independentemente do processo de desenvolvimento de software adotado;

VII - sempre que possível, metodologias e práticas ágeis deverão ser priorizadas em detrimento das práticas tradicionais de engenharia de software, assegurando a adoção de ciclos de desenvolvimento mais curtos e a entrega de valor constante para a organização; e

VIII - sempre que necessário deve ser aplicado o respectivo processo de capacitação de gestores e usuários para nivelamento de conhecimentos em relação aos sistemas e aplicações corporativas do FNDE.

SUBSEÇÃO XIII - DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS

Art. 27. O processo de gerenciamento de segurança da informação, proteção de dados e privacidade deve buscar equilíbrio entre o estabelecimento de políticas fortes, capacidade de auditoria, capacitação e implementação de processos de gestão de riscos, considerando as seguintes diretrizes específicas:

I - toda e qualquer informação e dado gerado, custodiado, manipulado, utilizado ou armazenado no FNDE deve ser considerado um ativo relevante para a organização, sendo objeto de proteção com vistas à preservação dos atributos de disponibilidade, integridade, confidencialidade e autenticidade, na forma das leis e das normas vigentes;

II - todo ativo de informação deve ser classificado e tratado segundo sua classificação, de maneira a receber adequada proteção durante todo seu ciclo de vida (criação, coleta, utilização, custódia e descarte);

III - todo acesso a dado deve ter a autorização expressa do gestor do dado, além da necessidade de assinatura de Termo de Responsabilidade para acesso a dados sensíveis, pessoais ou sigilosos, na forma da legislação vigente;

IV - as medidas e controles de segurança devem ser estabelecidos considerando a relevância dos ativos, os níveis de risco associados, o ambiente, o valor e a criticidade das informações e dos dados, de forma proporcional e balanceada, visando sempre a prevenção à ocorrência de incidentes;

V - pessoas e aplicações devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma determinada tarefa, tendo como condição essencial a ciência expressa quanto às responsabilidades e compromissos decorridos deste acesso e o conhecimento das penalidades cabíveis pela inobservância das regras previstas;

VI - todos os usuários são individualmente responsáveis pela segurança dos ativos sob sua custódia e pelo uso e guarda de suas credenciais de acesso, vedada a exploração de eventuais vulnerabilidades que, assim que identificadas, devem ser imediatamente comunicadas às instâncias competentes;

VII - todos os contratos de prestação de serviços firmados pelo FNDE deverão conter cláusula específica sobre a obrigatoriedade de conhecimento e atendimento às diretrizes e normas vinculadas a gestão de segurança da informação, privacidade e proteção de dados, incluindo, sempre que possível, a assinatura de termo de responsabilidade pelas empresas contratadas e de termo de ciência pelos colaboradores diretamente envolvidas na execução dos serviços contratados.

§1°. As diretrizes e objetivos dos processos de gestão de segurança da informação, privacidade e proteção de dados devem ser consolidadas em Política de Segurança da Informação e de Comunicações, que se desdobrará em normas complementares e procedimentos operacionais para cada segmento específico relevante.

§2°. A gestão de segurança da informação deve ser suportada por ações e métodos que visem a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento das informações e dados, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, táticos e operacionais.

§3°. O uso dos recursos de Tecnologia da Informação e Comunicação disponibilizados pelo FNDE deve ser passível de monitoramento e auditoria, incluindo a análise regular de registros de eventos (log) com a aplicação, sempre que viável, de softwares utilitários específicos para monitoramento do uso de sistemas computacionais.

§4°. Sempre que possível deverão ser implementados e mantidos mecanismos que permitam a rastreabilidade dos recursos de TIC através de estratégias como trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para toda a rede e sistemas corporativos.

§5°. Deve ser instituído o Subcomitê de Segurança da Informação, como estrutura multidisciplinar subordinada ao Comitê de Governança Digital, para tratar dos assuntos específicos relacionados ao conjunto de políticas, processos, procedimentos e controles relacionados à segurança da informação, segurança cibernética, privacidade e proteção de dados no âmbito do FNDE.

§6°. Os processos de gestão de segurança da informação, privacidade e proteção de dados devem ser periodicamente avaliados com relação ao grau de implementação de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

SUBSEÇÃO XIV - DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 28. Deve ser implementado um Programa de Gestão de Continuidade de Negócio (PGCN) visando estabelecimento de práticas e critérios de análise de impacto, contingência, recuperação e resiliência dos serviços e ambientes de TIC, de modo a mitigar a possibilidade de interrupção das atividades da Autarquia causada por desastres ou falhas em recursos de TIC que suportam processos operacionais da organização.

§1°. O Programa de Gestão de Continuidade de Negócio - PGCN definirá os objetivos, princípios e diretrizes de alto nível que traduzirão a visão estratégica organizacional para a gestão da continuidade de negócio, além de orientar a elaboração dos planos correlatos, a análise de riscos e de impacto, as estratégias de continuidade segundo a cadeia

de valor integrada, os procedimentos e as ações relacionadas ao retorno do ambiente ao seu estado de normalidade.

§2°. A resiliência dos serviços e ambientes de TIC deve ser testada e revisada periodicamente, para refletir as mudanças tanto da estratégia corporativa quando das infraestruturas físicas e lógicas de TIC correlacionadas.

§3°. Os processos de gestão de da continuidade do negócio devem ser periodicamente avaliados com relação ao grau de cumprimento de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

SUBSEÇÃO XV - DA GESTÃO DE RISCOS, INTEGRIDADE, CONTROLE INTERNO E CONFORMIDADE

Art. 29. Deve ser executado um processo de gestão dos riscos de TIC no qual estejam estabelecidos papéis e responsabilidades, estratégias gerais e critérios de identificação e avaliação de riscos, preferencialmente como parte do processo institucional de gestão de riscos, considerando as seguintes diretrizes específicas:

I - o fomento à cultura de gestão de riscos como processo essencial de apoio a implementação de estratégias, planos, projetos e tomada de decisões para consecução dos objetivos estratégicos organizacionais e setoriais;

II - riscos de TIC devem ser identificados, mapeados, analisados, avaliados, tratados, monitorados e comunicados de forma contínua;

III - estabelecimento de critérios para tratamento dos riscos relacionados à TIC, considerando-se os aspectos legais, financeiros, operacionais, tecnológicos, negociais e de preservação da imagem da instituição; e

IV - atuação sistemática da gestão de riscos de TIC concomitantemente ao monitoramento da execução da estratégia, dos planos táticos e operacionais e das ações e projetos.

§1°. Deve ser elaborada e mantida uma política de gestão de riscos em Tecnologia da Informação, que definirá os objetivos, os princípios e as diretrizes de alto nível oriundos da visão estratégica organizacional para a gestão de riscos de TIC - orientando a elaboração de normas e procedimentos correlatos.

§2°. Os processos de negócio críticos da Autarquia devem ter seus riscos de TIC mapeados, analisados e avaliados. Devendo ser produzido e mantido atualizado um plano de tratamento e resposta aos riscos avaliados, envolvendo ações para mitigação, transferência, eliminação ou aceitação de riscos, conforme os critérios a serem estabelecidos.

Art. 30. A integridade em TIC observará as seguintes diretrizes específicas, associadas à gestão de riscos:

I - definição e implementação de controles de integridade para prevenção, detecção e remediação de ocorrências e atos indesejados;

II - garantir a prestação de contas de forma transparente, sistemática e ativa;

III - assegurar a integridade de dados e informações;

IV - assegurar a integridade dos processos de governança e gestão de TIC, em aderência às boas práticas vigentes;

V - desenvolver práticas e mecanismos para garantir a proteção da disponibilidade, da confidencialidade, da acessibilidade e da integridade de dados e

informações corporativas, com a definição de padrões específicos e atualizados de segurança para as bases de dados internas, para preservar os processos e a imagem da instituição; e

VI - assessorar e subsidiar, no que couber, as instâncias internas competentes visando implementar ações de melhoria contínua das práticas de gestão e governança em TIC.

Parágrafo único. As soluções digitais de uso corporativo devem considerar aspectos relativos à ética, integridade, inclusão social, responsabilidade socioambiental, eficiência, eficácia, legalidade, sustentabilidade, segurança da informação, empatia, idoneidade, além do respeito à diversidade e valorização das pessoas.

Art. 31. Os controles internos de TIC devem observar as seguintes diretrizes específicas, associadas à gestão de riscos e à integridade:

I - monitoramento da conformidade, do desempenho e das práticas de governança e gestão de TIC por meio da implementação de controles adequados e promoção de ações corretivas quando desvios forem identificados;

II - assegurar que as estratégias definidas e os normativos formulados estejam sempre em consonância com a legislação, as normas e os padrões vigentes; e

III - medir continuamente a maturidade das práticas de gestão e governança através da autoavaliação ou por meio da contratação de consultorias especializadas, para garantir que os processos internos de TIC estejam fornecendo o valor esperado para as partes interessadas internas ou externas.

Art. 32. Os processos de gestão de riscos, integridade, controles internos e conformidade devem ser periodicamente avaliados com relação ao grau de cumprimento de suas práticas, bem como avaliação dessas práticas quanto ao seu grau de eficiência, eficácia e efetividade de modo a subsidiar aplicação de ajustes e sua melhoria contínua.

CAPÍTULO VI - DOS PAPÉIS E DAS RESPONSABILIDADES

Art. 33. O gestor de TIC é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de Tecnologia da Informação e Comunicação, devendo, diretamente ou sob delegação regimental, assessorar o Comitê de Governança Digital no exercício de suas competências, provendo todas as informações de gestão para a tomada de decisão das instâncias superiores, competindo-lhe ainda:

I - elaborar o plano de monitoramento de governança e gestão de TIC;

II - elaborar relatórios de acompanhamento dos controles e indicadores definidos;

III - propor normativos específicos de apoio à Governança Digital e aos seus subdomínios;

IV - propor alterações nesta Política de Governança Digital; e

V - conscientizar os demais agentes públicos internos sobre os objetivos estratégicos de TIC e suas responsabilidades em cada processo ou prática relacionada.

Art. 34. Compete à alta administração, através do Comitê de Governança Digital:

I - aprovar, manter e revisar a Política de Governança Digital;

II - avaliar, direcionar e monitorar as normas e ações de governança e gestão de TIC; e

III - estabelecer as metas, os indicadores e os ciclos de avaliação do grau de maturidade em governança e gestão de TIC e realizar a análise crítica das práticas envolvidas.

Parágrafo único. Outras competências e atribuições específicas para o Comitê de Governança Digital e seus subcomitês poderão ser definidas em seus respectivos instrumentos de criação.

CAPÍTULO VII - DOS RECURSOS, DO MONITORAMENTO E DA ATUALIZAÇÃO DA POLÍTICA

SEÇÃO I - DOS RECURSOS

Art. 35. A Política de Governança Digital do FNDE deve ser considerada instrumento essencial para o sucesso das estratégias e dos projetos de Tecnologia da Informação e Comunicação, devendo os recursos necessários para a sua devida instrumentalização serem considerados sempre em conjunto com as demandas de TIC propriamente ditas.

SEÇÃO II - DO MONITORAMENTO E DA ATUALIZAÇÃO DA POLÍTICA

Art. 36. Esta POLÍTICA deve ser revisada e atualizada, no máximo, a cada 2 (dois) anos.

Parágrafo único. A devida publicidade das alterações deste normativo e publicações relacionadas a este instrumento deve ser assegurada para todas as partes interessadas envolvidas.

CAPÍTULO VIII - DAS DISPOSIÇÕES FINAIS

Art. 37. As normas, os processos e os procedimentos mínimos necessários para implantação desta Política devem ser definidos gradualmente no prazo máximo de 180 (cento e oitenta) dias após sua publicação.

Parágrafo único. O Comitê de Governança Digital estabelecerá a priorização das normas e processos de implantação desta política conforme as diretrizes corporativas e a capacidade interna da Diretoria de Tecnologia e Inovação.

Art. 38. As exceções e os casos omissos devem ser submetidos à apreciação do Comitê de Governança Digital para eventual alteração, na forma do seu regimento interno.