



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES

RESOLUÇÃO NORMATIVA Nº 4/2021 - CGRC (11.24.10.03)

Nº do Protocolo: 23077.062453/2021-74

Natal-RN, 09 de junho de 2021.

Institui a Política de Gerenciamento de Serviços de Tecnologia da Informação na Universidade Federal do Rio Grande do Norte.

O VICE-PRESIDENTE DO COMITÊ DE GOVERNANÇA, RISCOS E CONTROLE DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE, usando das competências previstas no artigo 23, §2º, incisos II, VII e XII, da Instrução Normativa Conjunta MP/CGU nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal,

CONSIDERANDO a Resolução No 039/2017-CONSAD, de 21 de setembro de 2017, que dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação da Universidade Federal do Rio Grande do Norte (PGTIC/UFRN);

CONSIDERANDO o inciso XIV, do art. 10, da Resolução 016/2017 o qual assinala que compete ao Comitê de Governança, Riscos e Controles aprovar propostas de políticas e diretrizes elaboradas pelo Comitê Gestor de Tecnologia da Informação (CGTI) e pelo Comitê Permanente de Segurança da Informação (CPSI); e

CONSIDERANDO a necessidade de disciplinar, institucionalizar e formalizar os processos de governança executados pelas equipes de TI da universidade.

RESOLVE:

Art. 1º Instituir a Política de Gerenciamento de Serviços de Tecnologia da Informação (PGSTI) da Universidade Federal do Rio Grande do Norte (UFRN).

**CAPÍTULO I
DISPOSIÇÕES PRELIMINARES**

**Seção I
Da finalidade**

Art. 2º Esta política tem por finalidade regulamentar, no âmbito da Universidade, práticas de gerenciamento de serviços de Tecnologia da Informação (TI) por meio do estabelecimento de diretrizes para sua implantação, contidas neste documento e em normas complementares, que servirão como base para a definição de macroprocessos a serem utilizados por todas as equipes de TI da UFRN.

Art. 3º As definições da aplicação de práticas e a institucionalização de seus macroprocessos de gerenciamento de serviços de TI tem como objetivos:

I - guiar os provedores de serviços de TI quanto às melhores práticas de gestão de serviços com foco na entrega de valor às partes interessadas com eficiência e efetividade;

II - estabelecer diretrizes para o cumprimento de práticas exigidas ou recomendadas por legislações federais e órgãos reguladores; e

III - promover uma cultura de gerenciamento de serviços de TI institucional, alinhada aos padrões internacionais de gestão de serviços mais relevantes.

Seção II Das definições

Art. 4º Para os efeitos desta Resolução, consideram-se:

I - valor: benefício, uso e importância percebida pelos consumidores dos serviços prestados;

II - risco: evento que possa comprometer a probabilidade de sucesso no alcance de um objetivo;

III - ativo de TI: bem, tangível ou intangível, que tenha valor para a instituição que possa contribuir para a entrega de um produto ou serviço de TI classificados em ativos de software, físicos ou informação, mas podem incluir outras categorias como as relacionadas a computação em nuvem e redes.

IV - partes interessadas: pessoas ou organizações com interesses ou envolvimento nos resultados de projetos, produtos, serviços e práticas;

V - produto de TI: arranjo de recursos organizacionais concebido para oferecer valor ao consumidor do produto, como por exemplo, um software;

VI - serviço de TI: meio de criar valor facilitando o alcance do resultado esperado pelo consumidor, evitando que precise controlar custos e riscos específicos;

VII - provedor de serviço de TI: responsável pelo gerenciamento do serviço de TI, o qual se responsabiliza pela gestão dos recursos, configuração para entrega dos serviços, garantias de acesso aos recursos pelos usuários, ações e níveis de serviço acordados e a sua melhoria contínua;

VIII - consumidor de serviço de TI: representa uma das partes interessadas no gerenciamento de serviços de TI, na qual as pessoas ou setores que recebem o valor produzido pelos serviços através do seu consumo;

IX - níveis de serviço: métricas que definem a qualidade esperada ou alcançada do serviços;

X - gerenciamento de serviço: busca garantir que os serviços prestados transformem uma demanda em valor ao consumidor do serviço;

XI - prática de gerenciamento de serviço: conjunto de recursos organizacionais concebidos para realizar um trabalho ou alcançar um objetivo;

XII - processo: conjunto de atividades relacionadas em uma sequência específica, evidenciando a dependência entre elas com o objetivo de transformar uma entrada em uma saída;

XIII - macroprocesso: processo definido para um domínio de uma prática ou fluxo de trabalho específico que contempla atividades pouco prescritivas e com baixo nível de detalhamento que permitam flexibilidade na sua operacionalização para atender seus objetivos;

XIV - processo de uma prática de gerenciamento de serviços de TI: especialização de um macroprocesso aplicado a um contexto específico;

XV - macroatividades: atividades ou grupo de atividades que representam ações genéricas ou pouco prescritivas em um processo com o objetivo de definir requisitos mínimos sem determinar a operacionalização deles;

XVI - papéis: conjuntos de responsabilidades e atividades de um domínio específico a serem assumidas por uma pessoa ou um grupo de pessoas dentro de um processo;

XVII - artefatos: documentos ou evidências concretas produzidos por uma atividade de um processo;

XVIII - indicadores de desempenho: mensuração, a partir de métricas ou combinação de métricas, que revela indícios relevante sobre impacto do valor produzido e entregue através de um processo;

XIX - radiador de informação: recursos visuais que auxiliam no compartilhamento e divulgação de informações entre partes interessadas no contexto de processos ou projetos;

XX - gestão visual: forma de gerenciar uma iniciativa baseada no uso de recursos visuais que contribuem com a colaboração e comunicação entre os participantes.

Seção III Do escopo

Art. 5º A regulamentação das práticas de gerenciamento de serviços de TI apresentadas nesta Resolução se aplicam a todas as unidades que gerenciam ativos de TI ou proveem algum serviço de TI.

Art. 6º São práticas de gerenciamento de serviços de TI contempladas nesta Resolução:

- I - gerenciamento de central de serviços;
- II - gerenciamento de requisição de serviços;
- III - gerenciamento de incidentes;
- IV - gerenciamento de problemas;
- V - gerenciamento de mudanças;
- VI - gerenciamento de configuração de ativos;
- VII - gerenciamento de ativos de TI;
- VIII - gerenciamento de riscos de TI;
- IX - gerenciamento de projetos de TI; e
- X - gerenciamento e desenvolvimento de software.

Art. 7º A regulamentação de cada prática de gerenciamento nesta Resolução é composta por:

- I - definições de objetivos e, quando couber, diretrizes específicas a serem atendidos, assim como responsabilidades do gestor da prática;
- II - instrumento normativo complementar que verse sobre os aspectos do inciso I deste artigo, quando necessário; e
- III - detalhamento de um macroprocesso, complementar a esta Resolução, composto por um fluxo mínimo de macroatividades, papéis, artefatos e indicadores de desempenho mínimos.

Parágrafo Único. O detalhamento do macroprocesso será disponibilizado pela Superintendência de Tecnologia da Informação (STI) em seu sítio eletrônico com fácil acesso e divulgação.

Art. 8º Não são contemplados pela regulamentação das práticas de gerenciamento nesta Resolução aspectos específicos de operacionalização de atividades, exceto em caso de exigência em legislação específica ou recomendação de órgãos controladores.

Seção IV Das diretrizes gerais

Art. 9º São perspectivas, que, de maneira transversal, devem ser observadas holisticamente em todas as práticas de gestão de serviços de TI:

- I - organizações e pessoas: compreendem elementos como papéis e responsabilidades, estruturas formais da organização, cultura, habilidades e competências mínimas;

II - informação e tecnologia: observam quais informações e conhecimentos serão necessários para criar, entregar e melhorar os serviços, além de quais tecnologias que poderão tornar o gerenciamento possível;

III - fluxos de valor e processo: observam as atividades, fluxos de trabalho, controles e procedimentos necessários para alcançar os objetivos; e

IV - parceiros e fornecedores: observam os relacionamentos com outras organizações envolvidas nas práticas do gerenciamento de serviços, assim como acordos e contratos com parceiros e fornecedores.

Art. 10. São diretrizes que devem nortear as práticas de gerenciamento de serviços de TI:

I - foque no valor: todas as atividades de um processo devem minimamente contribuir, direta ou indiretamente, com a entrega de valor às partes interessadas, especialmente aos consumidores dos serviços;

II - comece onde está: o desenvolvimento de melhorias de um processo ou a implantação de um novo deve buscar o aproveitamento de todos os elementos atuais que já contribuem com a entrega de valor e gradativamente evoluindo-os para atender às normas desta Resolução;

III - progrida iterativamente e com feedback: sempre que possível ações e entregas devem ser subdivididas em partes menores, planejadas e executadas em curtos períodos, e cada período incorporando melhorias identificadas nos anteriores;

IV - colabore e promova visibilidade: deve-se proporcionar um ambiente colaborativo entre as partes interessadas que propicie a co-criação de valor nos serviços prestados desde a concepção até o consumo, assim como garantir a transparência das informações através do uso de radiadores de informações ou outros artifícios usados na gestão visual de processos;

V - pense e trabalhe holisticamente: de acordo com a complexidade e setores envolvidos no gerenciamento dos serviços, deve-se observar e buscar a colaboração de todas as áreas da organização relacionadas para contribuir com a criação de valor prestado com o serviço;

VI - mantenha simples e prático: deve-se priorizar a simplificação na criação de valor dos serviços, no qual privilegia-se a minimização de custos das partes interessadas enquanto garante-se a compreensão e a entrega de valor;

VII - otimize: seguindo o princípio da eficiência, deve-se buscar a otimização de forma holística, iterativa e contínua considerando os aspectos mencionados no art. 9º, assim como observar as restrições submetidas e os recursos disponíveis;

VIII - automatize: considerando um processo otimizado, a tecnologia deve ser usada para auxiliar na automatização de passos de processos das práticas que possam dispensar a intervenção humana de maneira a contribuir com a eficiência do seu desempenho;

IX - meça e acompanhe indicadores: a melhoria contínua deve ser observada a partir da evolução de indicadores de desempenho de processos, definidos a partir de métricas relevantes sendo aferidas e acompanhadas regularmente; e

X - revise e atualize processos: deve-se garantir que as documentações complementares a esta Resolução, como o detalhamento dos macroprocessos possam ser facilmente alteradas e publicizadas, considerando as modificações resultantes das revisões periódicas mencionadas no art. 13, inciso II.

Art. 11. Deve haver registro formal no SIGRH de todas as pessoas que atuam em equipes de TI na UFRN de maneira que esse dimensionamento possa auxiliar no planejamento de ações institucionais na melhoria de gestão de serviços de TI da Universidade.

Seção V

Da implantação das práticas de gerenciamento de serviços de TI

Art. 12. A implantação da gestão de cada prática requer que o provedor de serviço observe o atendimento aos elementos citados no artigo art. 7º.

Parágrafo único. O provedor de serviço de TI poderá especializar o macroprocesso, inclusive expandindo-o, desde que seu processo de gerenciamento de serviços de TI garanta o cumprimento descrito no caput deste artigo.

Seção VI Das responsabilidades

Art. 13. Compete à STI:

I - definir e publicizar os detalhes dos macroprocessos especificados no art. 7º, III desta Resolução;

II - garantir a revisão dos macroprocessos anualmente com o intuito de assegurar sua melhoria contínua;

III - definir os esquemas de classificação e categorização citados nesta Resolução, bem como os sistemas a serem utilizados pela UFRN nos processos de gerenciamento de serviços de modo a promover a cultura de gerenciamento de serviços de TI institucional, conforme determinado no inciso III, do art. 3º; e

IV - definir como será feito o registro dos membros das equipes de TI das unidades.

Art. 14. Compete às unidades provedoras de serviço de TI implantar e gerenciar as práticas compatíveis com seus serviços prestados, conforme especificado no art. 7º.

§ 1º Compete ao diretor de cada unidade que gerencia serviços de TI registrar formalmente todos os participantes da equipe de TI da unidade, bem como designar um gestor para cada prática de gerenciamento de serviço de TI;

§ 2º O papel de gestor de práticas de gerenciamento de serviços de TI diferentes poderá ser acumulado pela mesma pessoa.

Art. 15. Compete ao gestor de uma prática de gerenciamento de serviço de TI:

I - garantir que o processo de gerenciamento associado à prática seja executado atendendo às diretrizes gerais e específicas desta Resolução;

II - em caso de especialização de macroprocessos de gerenciamento de serviços de TI, garantir a documentação e publicação do processo específicos da unidade;

III - providenciar resultados de indicadores dos processos e evidências de artefatos em caso de auditoria solicitada; e

IV - seguir as demais orientações definidas, especificamente, em cada prática para esse papel.

Art. 16. Compete à Secretaria de Governança Institucional monitorar a aplicação das práticas de gerenciamento de serviços de TI.

Seção VII Fundamentações legais e normativas

Art. 17. As referências legais e normativas utilizadas para a elaboração dos processos de gerenciamento de serviços de TI da UFRN são apresentadas no Anexo I.

CAPÍTULO II DAS PRÁTICAS DE GERENCIAMENTO DE SERVIÇOS DE TI

Seção I Gerenciamento da Central de Serviços

Art. 18. A prática de gerenciamento de central de serviços visa coletar as demandas para requisições de serviço e resolução de incidentes, devendo ser o ponto único de entrada e contato dos usuários com as

equipes de TI.

Art. 19. São diretrizes específicas da prática de gerenciamento da central de serviços:

I - deve ser definido e publicizado os canais que serão utilizados para interação com os usuários, tais como telefone, e-mail, aplicativos de mensagens, cujas solicitações devem ser registradas em um sistema de chamados independente do meio utilizado;

II - deve ser utilizado um sistema de chamados único em toda a UFRN;

III - as atividades da central de serviços incluem tanto o atendimento remoto quanto presencial, devendo fazer uso de tecnologias que melhorem a qualidade dos serviços prestados e minimizem a necessidade de deslocamento físico;

IV - o atendimento prestado deve ir além de apenas resolver o problema técnico diretamente indicado pelo usuário, devendo-se analisar de fato o que ele precisa para que sejam fornecidas as explicações necessárias e dado o encaminhamento correto;

V - devem ser definidos quais atendimentos precisam ser feitos diretamente pela central de serviços e quais devem ser escalados para outras equipes.

VI - a equipe da central de serviços não precisa ter conhecimentos aprofundados nas tecnologias a que dão suporte, devendo possuir habilidades em outras áreas relacionadas ao comportamento humano, como facilidade de comunicação, empatia, entre outras.

VII - a equipe da central de serviços deve ter visão geral dos principais processos de negócios da instituição para entender melhor o impacto que os incidentes e as requisições podem ter na geração de valor para a instituição a fim de possibilitar a priorização e o escalamento das demandas de modo mais eficiente.;

VIII - deve haver forte colaboração entre a equipe da central de serviços e as demais equipes de TI da unidade por meio, principalmente, de interações recorrentes para facilitar o compartilhamento de conhecimento;

IX - deve ser incentivada a utilização de ferramentas que permitam o autoatendimento, bem como a automação de tarefas, gerando como uma de suas consequências a redução de esforço na equipe para que seja possível aprimorar a experiência do usuário quando o contato pessoal for necessário;

X - deve ser definido e divulgado à comunidade de usuários qual o horário de atendimento da central de serviços;

XI - deve haver monitoramento constante das atividades da central de serviços, incluindo a definição e acompanhamento de indicadores, especialmente, por meio do uso de radiadores de informações, como por exemplo, painéis e dashboards;

XII - deve ser mantida uma base de conhecimento de fácil acesso e colaboração entre equipes de TI e central de serviços para apoiar o atendimento às demandas;

XIII - deve ser definido um mecanismo para coleta do feedback sobre o atendimento às demandas dos usuários com o objetivo de aferir a efetividade do valor prestado;

XIV - a central de serviços deve sempre ser informada sobre a entrada de novos serviços ou mudanças nos serviços existentes;

XV - a central de serviços deve fornecer feedback para as demais equipes de TI da unidade e tentar identificar situações atípicas que justifiquem avaliação especial; e

XVI - a gestão do conhecimento deve avaliar a relação de eficiência e desperdício entre as abordagens de compartilhamento de conhecimento por meio da documentação e o compartilhamento do conhecimento tácito das equipes.

Art. 20. São responsabilidades específicas do gestor do processo da central de serviços:

I - definir os meios a serem usados para interação com os usuários; e

II - garantir que todas as solicitações sejam registradas no sistema de chamados.

Seção II

Gerenciamento de requisição de serviço

Art. 21. A prática de gerenciamento de requisição de serviço visa suportar a qualidade acordada de um serviço por meio do tratamento de todas as requisições pré-definidas e iniciadas pelo usuário de um modo eficaz e amigável.

Art. 22. A requisição de serviço consiste na solicitação de um usuário ou de algum representante autorizado pelo usuário que inicia uma ação de serviço acordada como parte normal da entrega do serviço.

Art. 23. São diretrizes específicas da prática de gerenciamento de requisição de serviço:

I - deve existir categorização única para todas as requisições de serviços de TI da UFRN, e cada unidade deve definir quais delas serão disponibilizadas, de acordo com os tipos de serviços oferecidos pela unidade, devendo cada unidade definir e publicizar seu catálogo de serviços;

II - as informações sobre as requisições de serviços devem ser mantidas em sistema único para toda a UFRN;

III - uma requisição de serviço é parte normal de entrega de serviço e não deve ser confundida com falhas ou degradação de serviço, que devem ser tratadas como incidentes e inclui:

a) Uma solicitação para ação de entrega de um serviço, por exemplo, substituir um toner, configurar um aplicativo, gerar um relatório;

b) Uma solicitação de informação, por exemplo, como criar uma conta de e-mail, qual o telefone de um setor;

c) Uma solicitação para o fornecimento de um recurso ou serviço, por exemplo, uma máquina virtual, fornecimento de um computador;

d) Uma solicitação de acesso a um recurso ou serviço, por exemplo, acesso a uma pasta na rede, acesso remoto via VPN; e

e) feedback, elogios e reclamações.

IV - considerando que algumas requisições de serviço incluem alterações em serviços ou seus componentes, deve ser definido quais tipos de requisição são consideradas como uma mudança padrão.

V - para cada tipo de requisição de serviço deve ser definido um fluxo de trabalho a ser seguido, incluindo os procedimentos para iniciação, aprovação, cumprimento, e gerenciamento, devendo esse passos serem bem conhecidos e testados, de modo a viabilizar estimativa do tempo de atendimento, e comunicação clara ao usuário de como se encontra o atendimento a sua solicitação em um dado momento;

VI - embora diferentes tipos de requisições tenham fluxos de trabalho diferentes, visando melhorar sua eficiência e manutenibilidade, deve-se procurar identificar modelos de fluxos que englobam diferentes tipos de requisições. Desse modo, quando novos tipos de requisições de serviço forem incorporadas ao catálogo de serviço, os modelos de fluxo já existentes devem ser reaproveitados sempre que possível;

VII - os fluxos de trabalho devem ser revistos periodicamente, em especial os associados aos seguintes tipos de requisições:

a) muito frequentes;

b) exigem esforço elevado para serem atendidos; e

c) possam comprometer significativamente a segurança da informação dos serviços prestados pela unidade.

VIII - deve-se automatizar o maior número possível das etapas dos fluxos de trabalho para atendimento das requisições de serviços;

IX - devem ser definidas regras referentes à aprovação das requisições de serviço, em especial, indicando quais devem ser atendidas sem necessidade ou com necessidade reduzida de aprovação;

X - as estimativas de tempo de atendimento devem ser definidas considerando uma visão realista do que a unidade consegue ofertar;

XI - devem haver fluxos de trabalho específicos para documentar e redirecionar solicitações que foram submetidas como requisição de serviço, mas de fato se tratam de incidentes ou mudanças; e

XII - as requisições que não puderem ser atendidas, seja porque o solicitante não atendeu as exigências para o direito de uso do serviço, seja pela falta de recursos computacionais disponíveis, ou qualquer outra razão, no encerramento do tratamento das requisições de serviço, deve constar a informação de não atendida.

Art. 24. São responsabilidades específicas do gestor do processo de requisição de serviços:

I - definir, em acordo com o gerente de mudanças, quais tipos de requisição são consideradas como uma mudança padrão;

II - definir o esquema de autorização para cada tipo de requisição;

III - garantir que os fluxos de trabalho sejam definidos para os diferentes tipos de requisição de serviço, e que sejam revisados periodicamente; e

IV - incentivar iniciativas de automação dos fluxos de trabalho associados às requisições.

Seção III Gerenciamento de incidentes

Art. 25. A prática de gerenciamento de incidentes visa minimizar o impacto negativo dos incidentes por meio da restauração da operação normal dos serviços tão rápido quanto possível.

Art. 26. Incidentes referem-se a interrupções não planejadas de um serviço ou degradação da sua qualidade.

Art. 27. São diretrizes específicas da prática de gerenciamento de incidentes:

I - os incidentes devem ser resolvidos dentro dos tempos adequados para atender aos acordos de nível de serviço;

II - todos os incidentes relacionados aos ativos deverão ser registrados, devendo conter pelo menos as seguintes informações:

a) identificador ou descrição do ativo;

b) data e hora da ocorrência;

c) categoria do incidente, conforme definido no inciso V.

III - devem ser mantidas informações que permitam acompanhar a evolução do atendimento de cada incidente de modo a possibilitar tanto o retorno ao usuário quanto a coleta de indicadores;

IV - as informações sobre os incidentes devem ser mantidas em sistema único para toda a UFRN, devendo ser o mesmo utilizado para o registro de requisições de serviços e permita o relacionamento com ICs, mudanças, erros conhecidos, e outras informações consideradas relevantes para a resolução do incidente.

V - os incidentes devem ser categorizados, podendo ser utilizado um modelo hierárquico para acomodar especificidades das unidades, mas pelo menos as categorias do nível mais alto devem ser comuns a toda a UFRN. Uma das categorias deve indicar incidentes de segurança da informação que envolvam a violação de dados pessoais.

VI - os incidentes devem ser priorizados, considerando pelo menos os critérios de gravidade e urgência;

VII - o esforço e consumo de recursos para resolução de incidentes deve considerar seu impacto, devendo haver procedimentos específicos para lidar com incidentes graves;

VIII - deve haver um processo separado para lidar com incidentes de segurança da informação e todos eles devem ser notificados ao Centro de Tratamento e Respostas a Incidentes de Segurança da Informação da UFRN (CeTRIS);

IX - deve haver mecanismos para facilitar a colaboração entre as pessoas atuando em um incidente;

X - para incidentes que demorem um tempo maior para serem resolvidos, deve ser garantido retorno para as partes interessadas, contendo informações sobre sintomas, impacto, ICs afetados, ações já realizadas e ações planejadas;

XI - quando houver pessoas suficientes na equipe de TI que viabilize a segregação de funções, elas devem ser separadas em diferentes grupos com as seguintes denominações e atribuições:

a) central de serviço: atendimento inicial ao usuário, requerendo nível menos especializado de conhecimento e com atribuição de resolver incidentes mais simples;

b) equipe de suporte: equipe com conhecimento técnico especializado, responsável por resolver incidentes mais complexos. Pode ser utilizado apenas um nível (Suporte de 2º nível) ou vários níveis (2º e 3º níveis), de modo a permitir maior segregação de funções.

XII - devem ser oferecidos mecanismos de orientação para que o próprio usuário resolva incidentes simples, e deve-se coletar informações sobre essas situações para auxiliar no monitoramento de indicadores e ações de melhoria;

XIII - os incidentes podem ser escalados entre os atores envolvidos, incluindo os parceiros e fornecedores, utilizando-se critérios de categoria e prioridade;

XIV - durante o processo de resolução de incidentes devem ser consultados os erros conhecidos e as soluções de contorno, além de tentar fazer a correlação do incidente sendo tratado com os demais incidentes;

XV - deve-se buscar automatizar algumas ações, principalmente, as relacionadas a diagnósticos e coleta de informações;

XVI - quando considerado pertinente, após analisar questões como recorrência do incidente e complexidade de solução, recomenda-se a definição de processos específicos com informações gerais de como investigar, diagnosticar e resolver tipos específicos de incidentes;

XVII - durante o encerramento de um incidente devem ser realizadas as seguintes atividades:

a) solicitar retorno do usuário sobre o atendimento, definindo-se um prazo de espera, devendo o chamado ser encerrado em definitivo após esse prazo, caso não se obtenha o retorno do usuário;

b) avaliar a pertinência de registrar junto ao incidente a solução adotada, sendo obrigatório o registro para incidentes envolvendo a violação de dados pessoais. Caso se opte pelo registro e uma nova solução tenha sido empregada, sua documentação deverá ser elaborada. O detalhamento das soluções já utilizadas deve ser mantido em uma base de conhecimento; e

c) avaliar se é necessário iniciar um processo de gerenciamento de problemas.

XVIII - devem ser definidos mecanismos para coletar periodicamente a percepção dos usuários referente ao processo de gestão de incidentes;

IX - caso o impacto do incidente seja muito elevado, deve ser considerado o acionamento da equipe responsável pela continuidade de TI;

XX - deverá ser feita, periodicamente, análise dos incidentes ocorridos, contemplando, pelo menos, o total de incidentes por categoria e a quantidade de incidentes atendidos fora dos tempos estimados.

Art. 28. São responsabilidades específicas do gestor do processo de gerenciamento de incidentes:

I - definir o esquema de priorização;

II - definir o esquema de classificação específico para a unidade, caso se adote na UFRN um modelo com essa possibilidade;

III - definir os critérios para escalamento dos incidentes; e

IV - garantir que durante o processo de gerenciamento de incidentes:

a) os erros conhecidos e as soluções de contorno sejam analisadas;

b) as novas soluções sejam documentadas na base de conhecimento;

c) seja fornecido feedback para as partes interessadas; e

d) o gestor de processo de continuidade de negócios seja acionado, quando necessário.

Art. 29. A equipe de TI de cada unidade deve se responsabilizar pelo registro e tratamento dos incidentes nos ativos da sua unidade.

Seção IV Gerenciamento de problemas

Art. 30. A prática de gerenciamento de problemas visa reduzir a probabilidade e o impacto dos incidentes por meio da identificação das causas dos incidentes reais e potenciais, bem como gerenciar soluções de contorno e erros conhecidos.

Art. 31. São definições específicas da prática de gerenciamento de problemas:

I - problema: causa ou potencial causa de um ou mais incidentes caracterizados por erros, falhas ou vulnerabilidades dos serviços, que não foram identificados e resolvidos antes de sua entrada em produção;

II - erro conhecido: problema que tem sido analisado, mas ainda não foi resolvido; e

III - solução de contorno: solução que reduz ou elimina o impacto de um incidente ou problema para o qual uma resolução completa ainda não está disponível, podendo também reduzir a probabilidade de sua ocorrência.

Art. 32. São diretrizes específicas da prática de gerenciamento de problemas:

I - diferentemente do gerenciamento de incidentes, que têm como foco restabelecer os serviços o mais rápido possível, o gerenciamento de problemas deve incluir investigação e análise para identificar as causas dos incidentes, desenvolver soluções de contorno e recomendar sua resolução definitiva, de modo a reduzir o número e o impacto dos incidentes futuros;

II - deve ser analisado o risco associado aos problemas, considerando sua probabilidade e impacto, de modo a priorizar os problemas e definir quais devem ser analisados;

III - o gatilho para iniciar o gerenciamento de problemas pode vir por meio da central de serviços após a resolução de um incidente, de alguma equipe interna, de ferramentas de monitoramento, entre outras,

devendo o processo atuar tanto de modo reativo, baseado em resolver incidentes, quanto pró-ativo, quando realiza análise de tendências, vulnerabilidades, entre outras ações, em busca de problemas;

IV - o gerenciamento de problemas é composto pelas fases de identificação do problema, controle do problema e controle de erro;

V - A fase de identificação do problema visa identificar e registrar os problemas por meio das seguintes atividades:

- a) realizar análise de tendências dos registros de incidentes;
- b) detectar questões repetidas e recorrentes feitas pelos usuários, central de serviço ou equipe de suporte;
- c) identificar os riscos de recorrência para os incidentes de maior relevância;
- d) analisar informações recebidas de parceiros e fornecedores;
- e) analisar informações recebidas dos times internos (testes, desenvolvedores, projetos, operações, entre outros);
- f) considerar outras fontes de informações consideradas relevantes; e
- g) registrar formalmente o problema.

VI - A fase de controle do problema visa realizar a análise do problema, das soluções de contorno e dos erros conhecidos, devendo considerar as causas que levam um incidente a acontecer, bem como as que contribuem para a sua duração e o impacto. Aplicam-se a esta fase:

- a) quando uma solução rápida não puder ser encontrada para o problema deve-se procurar descobrir e registrar formalmente uma solução de contorno. Caso já exista uma solução de contorno documentada, ela deve ser revisada, e possivelmente melhorada, depois que a fase de análise do problema estiver concluída;
- b) uma solução de contorno pode se tornar uma forma permanente de lidar com o problema quando a avaliação do custo benefício não justifica uma solução definitiva. Nesses casos, o problema permanece com o status de erro conhecido; e
- c) cada solução de contorno deve incluir clara definição das situações para as quais ela se aplica.

VII - a fase de controle do erro visa encontrar uma solução definitiva para os problemas, compreendendo as seguintes atividades:

- a) identificar solução permanente para o problema que pode resultar em uma requisição de mudança;
- b) analisar os erros conhecidos que ainda não foram solucionados, reavaliando o impacto, a efetividade das soluções de contorno e a viabilidade de implementar eventuais soluções definitivas já identificadas; e
- c) realizar o registro formal da solução definitiva, caso seja encontrada.

VIII - os registros formais citados nos incisos III, IV e V podem corresponder a uma documentação usando arquivos, como planilhas, por exemplo, mas recomenda-se que sejam feitos em um sistema de chamados, de preferência utilizando sistema único para toda a UFRN. Caso tal sistema não possua uma base de conhecimento integrada, devem ser registradas informações para permitir a relação entre os incidentes e problemas registrados no sistema e as informações na base de conhecimento. O registro dos erros conhecidos e das soluções de contorno devem ser feitos na base de conhecimento;

IX - quando o registro do problema referido na fase identificação do problema for feito em um sistema de chamados, não se deve transformar chamados de incidentes em problemas. O chamado de incidente deve ser encerrado e um novo chamado deve ser aberto como problema e vinculado ao incidente que o originou;

X - os problemas devem ser categorizados, podendo ser utilizado um modelo hierárquico para acomodar especificidades das unidades, mas pelo menos as categorias do nível mais alto devem ser comuns a toda a UFRN; e

XI - os problemas devem ser priorizados, considerando pelo menos os critérios de gravidade e urgência.

Art. 33. São responsabilidades específicas do gestor do processo de gerenciamento de problema:

I - definir o esquema de priorização;

II - definir o esquema de classificação específico para a unidade, caso se adote na UFRN um modelo com essa possibilidade; e

III - garantir que durante o processo de gerenciamento de problemas:

a) as soluções de contorno e as soluções definitivas sejam registradas;

b) a análise do problema inclui avaliação das soluções já registradas, sejam de contorno ou definitivas; e

c) sejam geradas requisições de mudanças para as soluções propostas.

Seção V

Gerenciamento de mudanças

Art. 34. O gerenciamento de mudança visa assegurar que a infraestrutura de TI permaneça alinhada aos requisitos do negócio, com menor risco possível, garantindo que todas as implementações e alterações que possam causar impacto na habilidade da área de TI sejam analisadas e planejadas.

Art. 35. São definições específicas da prática de gerenciamento de mudanças:

I - mudança: qualquer adição, alteração ou remoção de algo que possa, direta ou indiretamente, afetar serviços e produtos de TI;

II - gerenciamento de mudança: processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que mudanças benéficas sejam feitas com o mínimo de interrupção aos serviços de TI;

III - registro de mudança: registro contendo os detalhes de uma mudança, no qual documenta-se o ciclo de vida de uma única mudança recebida, mesmo para as rejeitadas posteriormente;

IV - Banco de Dados de Gerenciamento de Configuração (BDGC): base dados que armazena as informações referentes aos ICs que sofrerão a mudança;

V - Comitê de Controle de Mudança (CCM): grupo responsável pela avaliação do impacto das mudanças, devendo ser composto, quando apropriado, pelos seguintes perfis: gerente de mudança, cliente, equipe de desenvolvimento e manutenção de aplicações, consultores, especialistas e técnicos, equipe de serviços e representantes dos contratantes;

VI - Revisão Pós Implementação (RPI): revisão para verificar se a mudança trouxe os resultados esperados ou para indicar ações que devem ser tomadas para correção se houver algum problema ou ineficiência; e

VII - autoridade de mudanças: pessoa ou grupo de pessoas responsável por autorizar a implantação de uma mudança.

Art. 36. São diretrizes específicas da prática de gerenciamento de mudanças:

I - garantir o equilíbrio entre proporcionar real valor adicional a partir das mudanças em serviços e produtos de TI e proteger os usuários dos efeitos adversos das mudanças;

II - garantir o registro e classificação das mudanças a partir da necessidade do cliente ou de erro identificado no gerenciamento de problema.

III - garantir que todas as mudanças sejam analisadas por pessoas que compreendam os riscos e benefícios esperados pela mudança;

IV - garantir que todas as mudanças sejam categorizadas como:

a) mudanças padrão: consideradas mudanças bem conhecidas, bem documentadas, de baixo risco e sem necessidade de autorização adicional;

b) mudanças normais: mudanças que necessitam ter sua implantação agendada, ser analisadas e autorizadas seguindo processos de acordo com o grau de risco associado, de modo que para baixos riscos deve-se tornar o processo mais prático e rápido, enquanto para riscos maiores deve-se adotar um processo mais robusto, garantindo a sua máxima eficiência; e

c) mudanças emergenciais: mudanças que devem ser implementadas assim que possível, como por exemplo correções de incidentes de segurança, de maneira que tipicamente dispensam agendamento de implantação e necessitam de procedimentos otimizados de análise e autorização.

V - garantir definição de quem serão as autoridades de mudanças para cada tipo definido no inciso IV deste artigo, e que as mudanças sejam autorizadas de acordo com seu tipo;

VI - garantir o repasse ao grupo técnico para o desenvolvimento de mudança, assegurando a existência dos recursos necessários e o monitoramento do desenvolvimento;

VII - garantir que mudanças não afetem negativamente aspectos da segurança da informação, em especial a privacidade dos dados, assegurando os direitos dos usuários garantidos por lei;

VIII - garantir que a implantação das mudanças seja autorizada pelas devidas autoridades de mudanças, assegurando que nenhum atraso desnecessário é adicionado ao processo;

IX - garantir planejamento para implantação de mudanças agendáveis, de maneira a assegurar comunicação efetiva, evitar conflitos e alocação dos recursos devidos;

X - garantir a Revisão Pós Implementação (RPI), cujo objetivo é realizar a avaliação de todas as mudanças implementadas após determinado período;

XI - garantir que a maioria dos erros identificados antes de serem corrigidos sejam filtrados, analisados e testados para depois serem implementadas correções no ambiente de produção;

XII - considerar que mudanças de baixa importância, por exemplo, alteração de senhas, sejam controladas por procedimentos definidos na central de serviço;

XIII - observar a importância do apoio do gerenciamento de configuração para dar suporte à avaliação de impacto, indicando os itens de configuração envolvidos na mudança;

XIV - observar o uso de uma Base de dados de Gerenciamento da Configuração (BDGC) que forneça os serviços e recursos relacionados ao item de configuração que sofrerá a mudança.

Art. 37. São responsabilidades específicas do gestor do processo de gerenciamento de mudanças:

I - receber, registrar, classificar e alocar prioridades para todas as requisições de mudanças e rejeitar qualquer mudança que seja totalmente impraticável;

II - preparar a agenda de mudanças que serão discutidas no Comitê de Controle de Mudanças;

III - decidir as pessoas que devem participar das reuniões do Comitê de Controle de Mudanças;

IV - presidir as reuniões do Comitê de Controle de Mudanças;

V - enviar as agendas de mudanças para a central de serviço;

VI - relacionar-se com as partes para coordenar a construção, testes e a implantação das mudanças;

VII - atualizar o log das mudanças em andamento;

VIII - revisar as mudanças implantadas para verificar se elas atingiram os objetivos propostos;

IX - fechar os registros de mudanças concluídas; e

X - indicar as pessoas ou grupo de pessoas que exercerão o papel de autoridade de mudanças.

Seção VI

Gerenciamento de configuração de ativos

Art. 38. A prática de gerenciamento de configuração de ativos de TI visa assegurar a disponibilização de informações precisas e confiáveis sobre a configuração dos ativos e seus itens de configuração (ICs), quando e onde necessário, garantindo tanto a informação sobre como cada IC está configurado bem como dos relacionamentos entre eles.

Art. 39. As diretrizes e responsabilidades sobre a prática de gerenciamento de configuração de ativos de TI devem ser integradas à prática de gerenciamento de ativos.

Seção VII

Gerenciamento de ativos de TI

Art. 40. A prática de gerenciamento de ativos de TI visa planejar e gerenciar o ciclo de vida dos ativos de TI de modo a ajudar a instituição a maximizar valor, controlar custos, gerenciar riscos, suportar a tomada de decisão em relação a compras, reuso, descarte, bem como atender a requisitos legais.

Art. 41. As diretrizes e responsabilidades sobre a prática de gerenciamento de ativos de TI devem ser integradas à prática de gerenciamento de configuração de ativos de TI.

Seção VIII

Gerenciamento de riscos de TI

Art. 42. A prática de gerenciamento de riscos de TI deve buscar garantir que a Universidade reconheça, avalie e trate os riscos associados aos serviços, produtos e ativos de TI da instituição, assegurando o equilíbrio entre controlar os riscos de potenciais ameaças à prestação de serviços de TI e aproveitar os benefícios de oportunidades da inovação tecnológica.

Art. 43. As diretrizes e responsabilidades sobre a prática de gerenciamento de riscos de TI são contempladas pela Resolução Deliberativa nº 01/2021-CGRC, de 27 de maio de 2021.

Seção IX

Gerenciamento de projetos de TI

Art. 44. A prática de gerenciamento de projetos de TI visa assegurar que os projetos de TI sejam planejados, executados, monitorados e encerrados com sucesso, garantindo a satisfação das partes interessadas.

Parágrafo único. No caso de projetos que envolvem desenvolvimento de software, algumas particularidades como o alto grau de incerteza dos requisitos e a dinamicidade do escopo são aspectos que devem levar a gestão do projeto a abordagens menos tradicionais, como adoção de práticas ágeis para garantir a entrega de valor.

Art. 45. As diretrizes e responsabilidades sobre a prática de gerenciamento de projetos de TI serão definidas em Resolução específica.

Seção X

Desenvolvimento de software

Art. 46. A prática do desenvolvimento de software visa garantir que os produtos de software atendam às necessidades das partes interessadas em termos de funcionalidade, confiabilidade, manutenibilidade,

conformidade e auditabilidade.

Art. 47. Os objetivos e diretrizes desta Resolução acerca do desenvolvimento de software abrangem todos os produtos de software institucionais construídos e usados pela UFRN.

Parágrafo único. Os softwares contemplados por esta Resolução estão restritos aos produtos que gerenciam dados institucionais por meio de fluxos de processos administrativos ou acadêmicos.

Art. 48. O serviço público digital é definição específica da prática de desenvolvimento de software, entendendo-se como procedimentos realizados por meio eletrônico entre a sociedade e a Administração Pública para cumprimento de deveres ou acesso a direitos que requeiram algum instrumento de interação, como por exemplo, formulários de requerimento, inscrição e cadastramento.

Art. 49. São diretrizes específicas da prática de desenvolvimento de software:

I - garantir a implementação de mecanismos de segurança da informação e privacidade de dados, em conformidade com a Lei Geral de Proteção a Dados Pessoais;

II - garantir a implementação de mecanismos de interoperabilidade entre sistemas institucionais e do Governo Federal, em conformidade aos Padrões de Interoperabilidade de Governo Eletrônico (arquitetura e-Ping);

III - no caso de softwares com interação com o usuário, garantir recursos de acessibilidade, em conformidade com o Modelo de Acessibilidade em Governo Eletrônico (eMAG);

IV - garantir a aplicação do princípio "pergunte uma vez", o qual busca otimizar o acesso às informações dos usuários de Serviços Públicos Digitais a partir da integração entre sistemas estruturantes do Governo Federal, evitando-se múltiplas solicitações ao cidadão da mesma informação;

V - garantir participação de representantes das áreas de negócio dos produtos de software nas atividades de detalhamento e priorização das demandas, além das definições de critérios de aceitação das entregas;

VI - considerar a possibilidade do produto de software ser desenvolvido institucionalmente ou adquirido externamente para entregar valor às partes interessadas, considerando as relações de custo, benefício e risco;

VII - garantir a comunicação adequada a todas às partes interessadas sobre mudanças realizadas nos produtos;

VIII - considerar a possibilidade de desenvolvimento do produto em parceria com outras organizações;

IX - garantir auditabilidade dos produtos de software assegurando fácil acesso e análise dos logs produzidos;

X - garantir manutenibilidade de código-fonte e configuração a partir de boas práticas da engenharia de software;

XI - utilizar prioritariamente arquiteturas de software que promovam o desacoplamento de soluções, sistemas e componentes;

XII - garantir que a gestão de identidade de usuários de softwares institucionais utilize a base de dados única da Universidade em conformidade com a Política de Gestão de Identidade da UFRN;

XIII - garantir que a propriedade intelectual dos produtos de softwares institucionais da UFRN seja assegurada a todos os envolvidos pela sua construção e realizada a partir do registro de software através dos devidos procedimentos formais; e

XIV - garantir que todos os softwares institucionais sejam de conhecimento da STI.

Art. 50. O gestor do processo de desenvolvimento de software deve garantir que todos os softwares institucionais construídos pela sua unidade sejam comunicados à STI.

CAPÍTULO III DISPOSIÇÕES FINAIS

Art. 51. O prazo para definição e implantação dos sistemas de informação citados nesta política, que serão de uso institucional, é de dois anos a partir da entrada em vigor desta Resolução.

Art. 52. Esta Resolução entra em vigor em 01 de julho de 2021.

JOSÉ DANIEL DINIZ MELO
Presidente

ANEXO I FUNDAMENTAÇÕES LEGAIS E NORMATIVAS CONSIDERADAS NA ELABORAÇÃO DESTA RESOLUÇÃO

1. Decreto nº 10.332, de 28 de abril de 2020 - institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.
2. Lei nº 14.129, de 29 de março de 2021, dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública.
3. Resolução no 039/2017, dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação da Universidade Federal do Rio Grande do Norte (PGTIC/UFRN).
4. Resolução no 017/2019-CONSUNI, de 19 de junho de 2019, aprova o Regimento Interno da Reitoria da UFRN, no qual especifica as atribuições e competências da Superintendência de Tecnologia da Informação.
5. Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2019-2022 da Universidade Federal do Rio Grande do Norte (UFRN).
6. Resolução nº 056/2011-CONSAD, de 15 de dezembro de 2011, que normatiza a criação do Comitê Gestor de Tecnologia da Informação - CGTI da Universidade Federal do Rio Grande do Norte UFRN, atualizada pela Resolução nº 053/2016-CONSAD, de 29 de setembro de 2016.
7. Portaria no 623 / 2020 - R, de 12 de maio de 2020, que institui o Comitê Gestor de Segurança da Informação da UFRN.
8. Resolução no 016/2017-CONSAD, de 04 de maio de 2017, que institui a Política de Gestão de Riscos da Universidade Federal do Rio Grande do Norte - UFRN e cria o Comitê de Governança, Riscos e Controles.
9. Decreto nº 8.638 de 15, de janeiro de 2016, que institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
10. ePING - Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.

(Assinado digitalmente em 09/06/2021 15:36)

JOSE DANIEL DINIZ MELO

PRESIDENTE
UFRN (11.00)
Matricula: 1202134

Para verificar a autenticidade deste documento entre em <https://sipac.ufrn.br/public/documentos/index.jsp> informando seu número: **4**, ano: **2021**, tipo: **RESOLUÇÃO NORMATIVA**, data de emissão: **09/06/2021** e o código de verificação: **ab95e6152c**

