Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais - Reitoria
Avenida Vicente Simões, 1.111, Nova Pouso Alegre, Pouso Alegre / MG, CEP 37553-465 - Fone: (35) 3449-6150

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SUL DE MINAS GERAIS, nomeado pelo Decreto de 12.08.2014, publicado no DOU de 13/08/2014, seção 2, página 4, e em conformidade com a Lei 11.892/08, considerando:

I. os princípios e diretrizes estabelecidos na Política de Gestão de Riscos do IFSULDEMINAS (publicada no Boletim de Serviço de maio de 2017);

II. a criticidade dos dados e informações sob custódia, temporária e permanente, do IFSULDEMINAS em meios digitais e as especificidades da gestão de recursos e dos riscos associados a eles;

III. as orientações da Norma Complementar 04, da Instrução Normativa 01 DSIC/GSI/PR;

IV. as diretrizes para gestão de riscos da ABNT NBR ISO 31000;

RESOLVE:

Instituir a Política de Gestão de Riscos de TI do IFSULDEMINAS.

CAPÍTULO 01 - DISPOSIÇÕES GERAIS

Art. 1º. Esta política tem por finalidade definir princípios e diretrizes para orientar a gestão de riscos de TI no IFSULDEMINAS, buscando assegurar que possíveis eventos danosos não impactem os objetivos institucionais, ao mesmo tempo que oportunidades sejam aproveitadas de forma sustentável.

Parágrafo único. Entende-se por objetivos institucionais o alcance dos resultados pretendidos pela instituição e esperados por seus usuários, seja através da estratégia, de programas e projetos, de serviços e processos de negócio ou de qualquer outra forma de atuação institucional.

Art. 2º. Esta política se aplica a todas as unidades de TI do IFSULDEMINAS, estendendo-se a outras unidades organizacionais que venham a fornecer soluções de TI, em conformidade com a Política de Governança de TI (Resolução Nº 76/2015, de 17 de dezembro de 2015).

Parágrafo único. É considerada solução de TI, nos termos da Resolução Nº 76/2015, de 17 de dezembro de 2015, o conjunto formado por elementos de TI e processos de negócio que se integram para produzir resultados que atendam às necessidades do IFSULDEMINAS e de suas unidades organizacionais.

Art. 3º. Esta política é uma extensão da Política de Gestão de Riscos do IFSULDEMINAS (publicada no Boletim de Serviço de maio de 2017) e tem como escopo a gestão de riscos de TI, não abrangendo a gestão de riscos de outras áreas de negócio da instituição e seus processos específicos.

Parágrafo único. Esta política se alinha e complementa a Política de Gestão de Riscos do IFSULDEMINAS (publicada no Boletim de Serviço de maio de 2017), definindo diretrizes e objetivos específicos para a gestão de riscos de TI, não substituindo as determinações daquela política.

Art. 4º. A gestão de riscos deve ser tratada como prioridade institucional e contar com a alocação de recursos necessários em todas as instâncias envolvidas.

Art. 5º. A área de TI e as Unidades Gestoras de Soluções (Política de Governança de TI - Resolução Nº 76/2015, de 17 de dezembro de 2015) devem disseminar a cultura da gestão de riscos, de forma que os servidores sejam incentivados a identificar riscos, vulnerabilidades e ameaças e a preveni-los e tratá-los adequadamente.

Art. 6º. É requisito básico desta política a segregação de funções críticas, de forma que haja separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente as funções ou atividades-

chave de autorização, execução, aprovação, registro, revisão, auditoria ou asseguração.

CAPÍTULO 02 - MODELO DE GESTÃO DE RISCOS

Art. 7º. A gestão de riscos de TI no IFSULDEMINAS baseia-se no Modelo de Três Linhas de Defesa, amplamente utilizado mundialmente.

Primeira linha de defesa	Segunda linha de defesa	Terceira linha de defesa
PROPRIEDADE	*SUPERVISÃO*	*GARANTIA*
proprietário do risco: gestão operacional	controle de riscos e conformidade: gestão estratégica	auditoria e asseguração: auditoria interna e externa

Art. 8º. A adoção do modelo tem por finalidade estabelecer uma organização efetiva de comunicação na gestão de riscos e controles, determinando os papéis e responsabilidades essenciais.

Art. 9º. A composição das linhas de defesa resume-se às camadas de propriedade, supervisão e garantia, respectivamente, a primeira, a segunda e a terceira linhas de defesa.

Art. 10. A primeira linha de defesa é a gestão operacional, que possui e gerencia os riscos, sendo responsável por:

I. identificar, avaliar, controlar e mitigar riscos, direcionando o desenvolvimento e a implementação de políticas internas e procedimentos que garantam que as atividades estão consistentes e alinhadas com os objetivos e metas definidos.
II. implementar ações corretivas para endereçar deficiências em processos e controles, manter controles internos efetivos e executar procedimentos de controle no dia a dia.
III. tratar eventos de riscos, que envolvem a concretização das probabilidades e com algum impacto aos objetivos institucionais, inclusive através da execução de ações de contingência, previamente definidas.
IV. manter os níveis de risco dentro dos critérios definidos para apetite e tolerância a riscos no IFSULDEMINAS.
V. definir indicadores de riscos chave, que permitam uma melhor comunicação dos níveis de riscos para a Instituição.
VI. construir sistemas e soluções que tenham como base a resiliência, de forma que, em caso de eventuais imprevistos, os danos sejam reduzidos e reversíveis.
VII. implementar e manter o processo de gestão de riscos e assegurar a suficiência, a eficácia e a eficiência de quaisquer controles.

Parágrafo único. Compõem a primeira linha de defesa, para os fins previstos nesta política, enquanto gestão operacional, as coordenações de TI dos Campi e da Reitoria.

Art. 11. A segunda linha de defesa é a supervisão de riscos e conformidade, que monitora os riscos e sua gestão, em conformidade com o apetite e a tolerância a riscos institucionalmente definidos, sendo responsável por:

I. facilitar e monitorar a implementação de práticas eficazes de gestão de riscos pela gestão operacional.
II. auxiliar os proprietários de riscos a encontrar níveis aceitáveis de exposição e a reportar adequadamente as informações relacionadas aos riscos à instituição.
III. reportar diretamente à alta direção os níveis de riscos e os riscos-chave, além de fazer recomendações a respeito da gestão de riscos na Instituição.
IV. garantir que a primeira linha de defesa seja adequadamente desenvolvida e operada.

Parágrafo único. Compõe a segunda linha de defesa, para os fins previstos nesta política, enquanto gestão estratégica, a Diretoria de Tecnologia da Informação (DTI).

Art. 12. A terceira linha é a auditoria interna ou externa, que proporciona asseguração independente, sendo responsável por:

I. avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos.
II. assegurar que os controles internos são ou não adequados para tratar os riscos que podem comprometer o alcance dos objetivos institucionais.
III. orientar as demais linhas de defesa quanto à adequação dos controles internos existentes e sua suficiência frente aos riscos que a instituição enfrenta ou possa vir a enfrentar.
IV. avaliar as exposições a riscos relacionadas à governança, às operações e aos sistemas de informação da instituição, em relação a: alcance dos objetivos estratégicos institucionais,

confiabilidade e integridade das informações financeiras e operacionais, eficácia e eficiência das operações e programas, salvaguarda dos ativos e conformidade com leis, regulamentos, políticas, procedimentos e contratos.
V. fornecer garantia sobre a eficácia da governança, gerenciamento de riscos e controles internos, incluindo a maneira pela qual a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento e controle de riscos.
VI. reportar ao os resultados da auditoria e seus respectivos níveis de asseguração ao Comitê de Governança, Riscos e Controles (CGRC).

Parágrafo único. Compõe a terceira linha de defesa, para os fins previstos nesta política, enquanto auditoria e asseguração, a Auditoria Interna e auditorias externas independentes.

Art. 13. Os riscos dos quais trata esta política são agrupados em três categorias:

I. Risco de entrega de valor: associado com a oportunidade de usar ou não recursos tecnológicos para melhorar a eficiência e a eficácia de processos de negócio ou como viabilizador para iniciativas de negócio.
II. Risco de entrega de projetos: associado com a contribuição de recursos de TI para novas ou melhoradas soluções de negócio, normalmente na forma de projetos e programas.
III. Risco de entrega de serviços: associado com todos os aspectos de desempenho de sistemas e serviços de TI, podendo trazer destruição ou redução de valor para a instituição.

CAPÍTULO 03 - PROCESSO DE GESTÃO DE RISCOS

Art. 14. A gestão de riscos de TI se dará através de um processo cíclico e contínuo, respeitando os princípios e diretrizes definidos nesta política, composto pelas seguintes atividades:

I. Definição de contexto
II. Identificação de riscos
III. Análise de riscos
IV. Avaliação de riscos
V. Tratamento de riscos
VI. Monitoramento e comunicação de riscos

Art. 15. Cabe à gestão operacional definir os processos de gestão de riscos a serem utilizados em seus serviços, projetos e estratégias, contando com a aprovação da gestão estratégica.

§ 1º. A gestão operacional poderá adotar processos de gestão de riscos diferentes para projetos, serviços ou outras iniciativas, a fim de melhor atender às especificidades de cada uma das atuações institucionais.

§ 2º. Oportunamente, o processo de gestão de riscos e seus resultados serão avaliados pela auditoria interna ou externa, que poderá fazer orientações para seu aprimoramento e, se necessário, correção de insuficiências.

Art. 16. A gestão de riscos deve ser incorporada nos processos e práticas de TI, de forma que as atividades sejam executadas como parte do trabalho cotidiano.

Art. 17. O processo de gestão de riscos de TI será baseado nas etapas de definição de contexto, identificação, análise, avaliação e tratamento dos riscos e monitoramento e comunicação de riscos, de acordo com a NBR 31.000, com as diretrizes e particularidades operacionais definidas neste documento, cabendo à gestão operacional fazer oportunas customizações e melhorias.

Art. 18. Todas as etapas do processo de gestão de riscos deverão contar com registro formal e consistente, que garanta a integridade, confidencialidade, autenticidade e disponibilidade das informações, a fim de permitir consultas a dados históricos, geração de relatórios e registro e consulta de lições aprendidas.

Definição de contexto

Art. 19. A atividade de definição de contexto tem por finalidade definir os parâmetros externos e internos a serem levados em consideração no processo de gestão riscos, além de estabelecer o escopo e os critérios de risco para as demais etapas do processo.

§ 1º. O ambiente externo ao Instituto, no qual ele se localiza, deve ser considerado a fim de esclarecer os objetivos e preocupações das partes interessadas externas para desenvolvimento dos critérios de risco, considerando aspectos tecnológicos, requisitos legais e regulatórios e percepções de partes interessadas.

§ 2º. Para que o processo de gestão de riscos esteja adequadamente alinhado aos aspectos do ambiente interno do Instituto, devem ser considerados: a estratégia, objetivos e metas, oportunidades,

tecnologias, infraestrutura, cultura, entre outros que possam afetar positiva ou negativamente o processo de gestão de risco.

§ 3º. O contexto no qual o processo de gestão de riscos é executado deve ser avaliado, a fim de, no mínimo, especificar os recursos requeridos, as responsabilidades e as autoridades, além dos registros a serem mantidos.

Art. 20. É considerado nível de risco, nos termos da Política de Gestão de Riscos do IFSULDEMINAS, a medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos.

§ 1º. O nível de risco deverá ser aferido através da multiplicação entre o impacto e a probabilidade de sua ocorrência.

§ 2º. O impacto refere-se às possíveis consequências do risco, caso ele venha a ocorrer.

§ 3º. A probabilidade consiste na medição do quão provável é a ocorrência do risco.

§ 4º. A título de exemplo, os níveis de risco definidos na tabela abaixo poderão ser utilizados para operacionalização do processo de gestão de riscos.

IMPACTO	Muito baixa	Baixa	Possível	Alta	Muito alta
Catastrófico	Risco moderado	Risco alto	RIsco crítico	RIsco crítico	RIsco crítico
Grande	Risco moderado	Risco alto	Risco alto	RIsco crítico	RIsco crítico
Moderado	Risco pequeno	Risco moderado	Risco alto	Risco alto	RIsco crítico
Pequeno	Risco pequeno	Risco moderado	Risco moderado	Risco alto	Risco alto
Insignificante	Risco pequeno	Risco pequeno	Risco pequeno	Risco moderado	Risco moderado

PROBABILIDADE

Art. 21. O apetite a riscos definido pelo CGRC, conforme previsto na Política de Gestão de Riscos, é considerado o principal indutor para critérios de risco no Instituto e deve ser interpretado da perspectiva das soluções de TI.

Art. 22. De forma complementar ao apetite a riscos, definido pelo CGRC, o IFSULDEMINAS não tolerará:

I. riscos que possam comprometer os dados em suas propriedades de disponibilidade, integridade, confidencialidade e autenticidade.
II. riscos que possam comprometer a sustentabilidade e a entrega contínua das soluções de TI, classificados como críticos ou que suportem processos de negócios críticos.
III. riscos que possam resultar em inconformidade legal ou regulamentar.
IV. riscos que possam comprometer os níveis de serviço acordados com a instituição para as soluções TI.
V. riscos que possam comprometer a integridade das equipes de TI, individual ou coletivamente.

Parágrafo único. Outros critérios de riscos deverão ser definidos pela gestão operacional e estratégica, de acordo com as particularidade das soluções de TI sob avaliação.

Art. 23. Cabe à gestão estratégica definir junto ao CGRC quais os níveis aceitáveis para tolerância a

riscos.

Identificação de riscos

Art. 24. A atividade de identificação de riscos tem por finalidade identificar fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas potenciais causas e consequências, considerando os objetivos institucionais e os processos críticos de negócio.

Parágrafo único. Convém que a identificação de riscos inclua o exame de reações em cadeia provocadas por consequências específicas, incluindo os efeitos cumulativos e em cascata.

Art. 25. A identificação de riscos deve ter por base os processos críticos de negócio, os quais podem possuir em sua cadeia de dependências soluções de TI.

§ 1º. Cabe à gestão estratégica, junto ao Comitê de Governança, Riscos e Controles, identificar quais os processos críticos de negócio.

§ 2º. Através dos processos críticos de negócio, a gestão operacional identificará quais soluções de TI compõem, direta ou indiretamente, a cadeia de dependência do processo.

Art. 26. A atividade de identificação de riscos deve ser absorvida nas etapas de outros processos, como no desenvolvimento, manutenção, auditoria, atualização e outras que envolvam soluções de TI, de forma que sempre haja um olhar atento para incertezas que possam comprometer um ativo.

Análise de riscos

Art. 27. A atividade de análise de riscos envolve a compreensão dos riscos, a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer.

§ 1º. A análise dos riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas.

§ 2º. As consequências podem ser expressas em termos de impactos tangíveis e intangíveis.

§ 3º. A análise dos riscos deve levar em consideração controles existentes e sua eficácia e eficiência.

§ 4º. A análise dos riscos deve levar em consideração a interdependência dos diferentes riscos e suas fontes.

§ 5º. A análise dos riscos deve identificar fatores que afetam as consequências e a probabilidade.
Avaliação de riscos

Art. 28. A atividade de avaliação de riscos tem por finalidade identificar a necessidade de tratamento do risco e sua prioridade, a partir da análise dos critérios de risco estabelecidos no contexto.

§ 1º. Invariavelmente, a decisão quanto ao tratamento dos riscos deve levar em consideração os requisitos legais e regulatórios.

§ 2º. Havendo necessidade, a avaliação de riscos pode indicar que seja realizada uma análise mais aprofundada.

Tratamento de riscos

Art. 29. A atividade de tratamento de riscos tem por finalidade selecionar e executar uma ou mais opções para modificar os riscos, suas probabilidades e/ou impactos.

Art. 30. Tratar riscos envolve um processo cíclico composto por:

I. avaliação do tratamento de riscos já realizado.
II. decisão se os níveis de risco residual são toleráveis.
III. se não forem toleráveis, a definição e implementação de um novo tratamento para os riscos.
IV. avaliação da eficácia desse tratamento.

Art. 31. O tratamento dos riscos deve-se dar através de uma das opções a seguir:

I. evitar o risco: decisão de não iniciar ou descontinuar a atividade que dá origem ao risco.
II. mitigar o risco: decisão no sentido de reduzir o risco, reduzindo sua probabilidade e/ou consequência, ainda que reste algum risco residual a ser avaliado e tratado.

III. aceitar o risco: decisão de seguir em frente, aceitando a probabilidade e o impacto potencial do risco.
IV. transferir ou compartilhar o risco: transferir ou compartilhar o risco com outras partes.

Parágrafo único. O tratamento do risco pode envolver ainda a sua retenção, a fim de permitir uma decisão consciente e bem embasada a posteriori.

Monitoramento e comunicação de riscos

Art. 32. A atividade de monitoramento de riscos deve ser parte do processo de gestão de riscos e parte das atividades cotidianas, contemplando a checagem e vigilância regulares e o registro consistente de informações.

§ 1º. Cabe à gestão operacional, com anuência da gestão estratégica, definir a forma com que o desempenho da gestão de riscos será medido e reportado.

§ 2º. Cabe à gestão operacional automatizar, sempre que possível e viável, o monitoramento dos níveis de riscos.

Art. 33. A atividade de comunicação de riscos deve ser realizada regularmente, nos formatos e frequências previamente definidos.

§ 1º. Cabe à gestão estratégica definir junto ao CGRC a frequência e o formato nos quais os níveis de riscos serão comunicados ao Comitê.

§ 2º. As comunicações devem se dar pelos meios oficiais e institucionais, a fim de permitir o acesso a dados históricos.

CAPÍTULO 04 - DISPOSIÇÕES FINAIS

Art. 34. Para questões não detalhadas nesta Política, devem ser consideradas as definições da Política de Gestão de Riscos do IFSULDEMINAS (publicada no Boletim de Serviço de maio de 2017).

Art. 35. Cabe à DTI recomendar ao CGRC, com anuência do CGTI, que esta política seja atualizada, sempre que necessário.

Art. 36. Esta portaria entra em vigor na data da sua publicação.