Ministério da Educação

Instituto Federal do Espírito Santo

RESOLUÇÃO DO CONSELHO SUPERIOR nº 38/2020,

DE 27 DE AGOSTO DE 2020

Institui a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação do Instituto Federal do Espírito Santo.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO ESPÍRITO SANTO – Ifes, no uso de suas atribuições regimentais, considerando os autos do Processo nº 23147.000703/2019-97, bem como, as decisões do Conselho Superior em sua 65ª. Reunião Ordinária de 27 de agosto de 2020,

RESOLVE: : Instituir a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º. Esta política tem por finalidade definir princípios e diretrizes para orientar a gestão de riscos de TIC no Instituto Federal do Espírito Santo - Ifes, buscando assegurar que possíveis eventos danosos tenham o impacto minimizado frente aos 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 TIC do Ifes, estendendo-se a outras unidades organizacionais que venham a fornecer soluções de TIC, em conformidade com a Política de Governança Digital, conforme Resolução CS nº 37/2020 de 27/08/2020.

Parágrafo único. É considerada solução de TIC, nos termos da Resolução CS nº 37/2020 de 27/08/2020, conjunto formado por elementos de tecnologia da informação, sistemas, serviços e bens que se integram para produzir resultados que atendam às necessidades do Ifes e suas unidades organizacionais.

Art. 3º. Esta política é uma extensão da Política de Gestão de Riscos, Governança e Controle Interno do Ifes (Resolução do Conselho Superior nº 21/2017 de 07 de agosto de 2017) e tem como escopo a gestão de riscos de TIC, não abrangendo a gestão de riscos de outras áreas de negócio da instituição nem

seus processos específicos, além de definir diretrizes e objetivos específicos para a gestão de riscos de TIC, não substituindo as determinações daquela política.

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

Art. 5º. A área de TIC e os Gestores de Soluções de TIC, definidos por ato do Reitor conforme disposto na PGD, devem disseminar a cultura da gestão de riscos de TIC, 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 II
MODELO DE GESTÃO DE RISCOS

Art. 7º. A gestão de riscos de TIC no Ifes baseia-se no Modelo de Três Linhas de Defesa.

Primeira linha de defesa	Segunda linha de defesa	Terceira linha de defesa
PROPRIEDADE	SUPERVISÃO	GARANTIA
Proprietário do risco: gestão operacional	Proprietário do risco: gestão operacional	Proprietário do risco: gestão operacional

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

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

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

I - Desenvolver e implementar procedimentos internos alinhados à política, quando houver, com propósito de identificar, avaliar, controlar e mitigar riscos de TIC;

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 por meio da execução de ações de contingência, previamente

definidas;

IV - Manter os níveis de risco de TIC dentro dos critérios definidos para apetite e tolerância a riscos no Ifes;

V - Definir indicadores de riscos de TIC 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 de TIC. Parágrafo único. Compõem a primeira linha de defesa, para os fins previstos nesta política, enquanto gestão operacional, as Unidades de TI dos Campi e da Reitoria.

Art. 11. A segunda linha de defesa é a supervisão de riscos de TIC e conformidade que monitora os riscos de TIC 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 de TIC pela gestão operacional;

II - Auxiliar os proprietários de riscos de TIC a encontrar níveis aceitáveis de exposição e a reportar adequadamente as informações relacionadas aos riscos de TIC à instituição;

III - Reportar diretamente à alta direção os níveis de riscos e os riscos-chave de TIC, além de fazer recomendações a respeito da gestão de riscos de TIC 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 (DRTI).

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 de TIC;

II - Assegurar que os controles internos são ou não adequados para tratar os riscos de TIC 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 de TIC 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, 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 de TIC;

VI - Reportar os resultados da auditoria e seus respectivos níveis de asseguração ao CGRC ou, na ausência deste, à Autoridade Máxima da Instituição.

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 III
PROCESSO DE GESTÃO DE RISCOS

Art. 14. A gestão de riscos de TIC 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 de TIC a serem utilizados em seus serviços, projetos e estratégias, contando com a aprovação da gestão estratégica. Parágrafo único. A gestão operacional poderá adotar processos de gestão de riscos de TIC diferentes para projetos, serviços ou outras iniciativas, a fim de melhor atender às especificidades de cada uma das atuações institucionais.

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

Art. 17. O processo de gestão de riscos de TIC 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 permita consultas a dados históricos, geração de relatórios e registro e consulta de lições aprendidas.

Seção I

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 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 de TIC 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 de TIC.

§ 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 de TIC do Ifes, 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. Os níveis de risco estão definidos na tabela abaixo e devem ser utilizados para operacionalização do processo de gestão de riscos.

Impacto						
	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
		Muito Baixa	**Baixa**	**Possível**	**Alta**	**Muito Alta**

Probabilidade

Art. 21. A tolerância a riscos definido pelo CGRC ou, na ausência deste, pela Autoridade Máxima da Instituição, 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 TIC.

Art. 22. De forma complementar a tolerância a riscos, conforme o art. 21, o Ifes 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 continua 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 TIC;

V - Riscos que possam comprometer a integridade das equipes de TIC, individual ou coletivamente;

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

Art. 23. Cabe à gestão estratégica definir junto ao CGRC ou, na ausência deste, a Autoridade Máxima do Órgão quais os níveis aceitáveis para tolerância a riscos.

Seção II

Identificação de Riscos

Art. 24. A atividade de identificação de riscos de TIC 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 de TIC deve ter por base os processos críticos de negócio, os quais possuem em sua cadeia de dependências soluções de TIC.

§ 1º. Cabe à gestão estratégica, junto ao Comitê de Governança, Riscos e Controles ou, na ausência deste, a Autoridade Máxima do Órgão identificar quais os processos críticos de negócio.

§ 2º. Através dos processos críticos de negócio, a gestão operacional identificará quais soluções de TIC 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 TIC.

Seção III

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 e a probabilidade de que essas consequências possam ocorrer.

§ 1º. A análise dos riscos pode ser qualitativa, 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.

Seção IV

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.

Seção V

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 será por meio de uma das opções a seguir:

I - Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;

II - Assumir ou aumentar o risco de maneira a perseguir uma oportunidade;

III - Remover a fonte de risco;

IV - Mudar a probabilidade;

V - Mudar as consequências;

VI - Compartilhar o risco (por exemplo, por meio de contratos, compra de seguros); VII - Reter o risco por decisão fundamentada.

Seção VI

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 frequência previamente definidos.

§ 1º. Cabe à gestão estratégica definir junto ao Comitê de Governança, Riscos e Controles ou, na ausência deste, a Autoridade Máxima do Órgão a frequência e o formato nos quais os níveis de riscos serão comunicados a estes.

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

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 34. Para questões não detalhadas nesta Política, devem ser consideradas as definições da Política de Gestão de Riscos do Ifes (Resolução do Conselho Superior nº 21/2017 de 07 de agosto de 2017).

Art. 35. Cabe à DRTI recomendar ao Comitê de Governança, Riscos e Controles ou, na ausência deste, a Autoridade Máxima do Órgão, com anuência do CGTI, que está política seja atualizada, sempre que

necessário.

Art. 36. Esta resolução entra em vigor na data de sua publicação

Jadir José Pela
Reitor - Ifes
Presidente do Conselho Superior