Política de Gestão de Riscos de TIC

UNIFESSPA | Centro de Tecnologia da Informação e Comunicação

Política de Gestão de Riscos de Tecnologia de Informação e Comunicação (TIC)

CTIC – Unifesspa
2020

Histórico de Revisão

Versão	Data	Autor	Descrição
1.0	20/06/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Versão Inicial
1.1	23/07/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Revisão e sugestões
1.1.1	30/07/2020	Vitor Castro (Direção CTIC)	Revisão e sugestões
1.2	03/08/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Consolidação
1.3	08/08/2020	Vitor Castro	Revisão e sugestões finais
1.4	10/08/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Consolidação Final
1.4	13/10/2020	CGD	Aprovação na 12ª Reunião do CGD

Sumário

1. Introdução

A ação e interação dos objetivos organizacionais junto com as incertezas dão origem ao risco, que se apresentam no dia a dia de todas as formas em quaisquer atividades desenvolvidas. Muitas vezes, o risco não se apresenta visível, sendo necessárias determinadas ações para identificá-lo; em outras situações o risco é proveniente de ações repentinas que fogem do controle humano, como no caso de eventos de causas naturais.

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, execução e da gestão contratual. O gerenciamento de Riscos de Tecnologia da Informação e Comunicação (TIC) tem por objetivo apresentar os principais ativos de tecnologia da informação e comunicação, assim como detalhar suas ameaças, vulnerabilidades, controles e riscos associados.

O presente documento institui a Política de Gestão de Riscos de Tecnologia da Informação e Comunicação (TIC) do Centro de Tecnologia de Informação e Comunicação (CTIC), pertencente a Universidade Federal do Sul e Sudeste do Pará (Unifesspa), e cria o Comitê de Riscos de TIC (CRTIC) e Diretoria de Riscos de TIC (DRTIC).

A presente Política de Gestão de Riscos de Tecnologia da Informação e Comunicação (TIC), referida apenas como Política de Gestão de Riscos na continuidade desse documento, tem como objetivo embasar os princípios, conceitos e os valores que norteiam o Plano de Gestão de Riscos de Tecnologia da Informação e Comunicação (TIC) do CTIC / Unifesspa, no processo de Gestão de Riscos de TIC. O referido Plano de Gestão de Risco de TIC também descreve o controle, gerenciamento, monitoramento, mensuração e o ajuste permanente dos riscos inerentes a cada um dos ativos e serviços, inclusive em situações de estresse, e foi concebido de modo a conferir transparência com relação às rotinas e o processo formal praticado pelos gestores no gerenciamento dos riscos.

1.1. Escopo da política de gestão de riscos

A Política de Gestão de Riscos de TIC consolida as definições, diretrizes, responsabilidades e áreas envolvidas para que sejam estabelecidas as práticas de gerenciamento dos riscos descritas, revisadas, estabelecidas e documentadas no Plano de Gestão de Riscos de TIC do CTIC/Unifesspa.

Esta política deve ser aprovada pelo Comitê de Governança Digital (CGD) e possuirá revisão bianual, ou, em menor prazo, quando o CGD considerar necessário. Casos não previstos nesta política devem ser levados extraordinariamente ao CGD. A normativa abrange as

áreas pertencentes ao Plano de Gestão de Riscos de TIC e todos os processos de gestão e controle do risco envolvidos geridos pelo CTIC/Unifesspa.

O Plano de Gestão de Riscos de TIC deve estar em conformidade e alinhado aos requisitos e políticas internas que fazem parte do escopo interno da organização o qual ele está sujeito, tanto do CTIC quanto a própria Unifesspa. A lista das principais políticas internas e planos estão listadas abaixo com seus respectivos períodos de atualização.

- PDI (Plano de Desenvolvimento Institucional), quadrienal;
- PDTIC (Plano Diretor de Tecnologia da Informação e Comunicação), bienal;
- Política de Gestão de Riscos de TIC, bienal;
- POSIC (Política de Segurança da Informação e Comunicação), anual;
- Política de uso dos recursos computacionais, quadrienal;
- Plano de integridade, anual;

2. Governança

É necessária uma abordagem sistemática de gestão de riscos que muda de organização para organização, assim como o nível de risco aceitável de cada uma, sendo que risco aceitável é o grau de risco que a organização está disposta a aceitar para concretizar seus objetivos. Além disso, faz-se necessário aumentar a capacidade de gerir o risco e otimizar o retorno. A metodologia utilizada para a construção do Plano de Risco de Gestão de Riscos foram as normas ABNT NBR ISO/IEC 27005:2019 e a norma ABNT NBR ISO 31000:2018.

As definições, diretrizes e vocabulários para os termos utilizados no Plano de Gestão de Risco de TIC do CTIC/Unifesspa abaixo foram referenciados e aplicados a partir das normas ABNT NBR ISO 31000:2018, norma ABNT ISO GUIA 73:2009 e norma ABNT NBR ISO/IEC 27005:2019. Os termos são: Segurança da Informação, Ameaça, Vulnerabilidade, Risco, Riscos de segurança da informação, Identificação de riscos, Impacto, Estimativa de riscos, Ações de modificação do risco, Comunicação do risco, Ação de evitar o risco, Retenção do risco, Compartilhamento do risco.

2.1. Estrutura

A área de TIC na Unifesspa é representada pelo CTIC, um órgão suplementar ligado a Reitoria (o organograma da Unifesspa pode ser visualizado no seguinte link: https://transparencia.unifesspa.edu.br/2-uncategorised/101-organograma-unifesspa.html). O Centro está organizado em 03 (três) divisões: Divisão de Sistemas de Informação (DISI), Divisão de Redes e Serviços de Internet (DIRSI), Divisão de Contratação em Tecnologia da Informação (DICTI), também conta com 03 (três) coordenadorias: Coordenadoria de Atendimento ao Usuário (CAU), Coordenadoria de Administração e Controle Patrimonial (CACP) e Coordenadoria de Governança em Tecnologia da Informação (CGTI), que possuem a função de prover apoio aos usuários dos serviços de TIC da Unifesspa, realizar o apoio administrativo, financeiro, patrimonial e auxiliar os processos finalísticos do CTIC, por meio do uso e implementação de práticas de Governança de TIC, respectivamente.

Respectivamente, essas divisões têm atribuições diretamente ligadas ao desenvolvimento, implantação e manutenção de sistemas, gerenciamento dos serviços de infraestrutura de TIC, e o apoio e planejamento às contratações de TIC.

Como órgão executivo, o setor de TIC atua alinhado às estratégias direcionadas pelo CGD que tem papel consultivo e deliberativo. O Comitê tem como competências: Promover a integração das estratégias da área de TIC e as estratégias organizacionais, apoiar a Administração Superior nos assuntos referentes às áreas finalísticas no âmbito de TIC da Unifesspa, propor e aprovar políticas e padrões relacionados às soluções de TIC, elaborar, aprovar e monitorar o Plano

Diretor de Tecnologia da Informação e Comunicação (PDTIC), implementar o gerenciamento do processo de contratação de bens e serviços de TIC, aderindo ao que determina à Instrução Normativa n° 04/2014 – STI/MPOG e sua posterior atualização através da IN 01/2019 do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital;

2.2. Escopo legal e regulamentações externas

A gestão de riscos é um processo para identificar, avaliar, administrar, controlar e monitorar potenciais eventos ou situações capazes de afetar o desempenho da instituição, buscando estabelecer uma garantia razoável quanto ao cumprimento de seus objetivos. Para fins de aplicação do Plano de Gestão de Riscos de TIC, serão considerados, no que couber, os conceitos estabelecidos por Instruções Normativas dos Órgãos competentes como o Ministério de Planejamento Orçamento e Gestão (MPOG) e a Controladoria Geral da União (CGU), Processos de Gestão de Riscos padronizados internacionalmente, amplamente utilizados pelo mercado e adotados pelas organizações nacionais como ABNT NBR ISO/IEC. A lista com os principais escopos legais, padrões e regulamentações externas utilizadas neste Plano de Gestão de Riscos de TIC estão listados abaixo.

- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016 (IN 01) CGU/MP, de autoria da Controladoria Geral da União (CGU) e do Ministério do Planejamento (MP), que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Processo de Gestão de Riscos da Norma ABNT NBR ISO/IEC 31000:2018 Gestão de Riscos;

- Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre Gestão de Riscos, Auditoria e Controles Internos no estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;

- Decreto nº 8.945, de 27 de dezembro de 2016, que regulamenta a Lei nº 13.303;

- Norma ABNT NBR ISO/IEC 31000:2018 Gestão de Riscos – Princípios e diretrizes: norma que fornece os princípios e diretrizes genéricas para qualquer indústria ou setor.

- Norma ABNT NBR ISO/IEC 31010:2012 Gestão de riscos – Técnicas de avaliação de riscos: norma que deve ser trabalhada em apoio à norma “ABNT NBR ISO 31000:2018 Gestão de Riscos – Princípios e diretrizes”. Descreve as diversas técnicas e ferramentas de análise de risco (ainda não traduzida pela ABNT).

- Norma ABNT NBR ISO/IEC 27001:2013 destinada à tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – requisitos. Apresenta e descreve os requisitos que devem ser implementados no estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI).

- Norma ABNT NBR ISO/IEC 27002:2013 destinada à tecnologia da informação – técnicas de segurança – código de prática para a gestão de segurança da informação. Apresenta as melhores práticas para uma gestão adequada da segurança da informação.

- ABNT NBR ISO/IEC 27005:2019 destinada à tecnologia da Informação – técnicas de segurança – gestão de riscos de segurança da informação. Apresenta as diretrizes para o gerenciamento dos riscos de segurança da informação, além de empregar os conceitos da norma ABNT NBR ISO 27001:2013.

- ABNT ISO GUIA 73:2009 Gestão de Riscos – Vocabulário: norma que apresenta as definições de termos genéricos relativos à gestão de riscos. Portaria nº 06/2019 CTIC/Unifesspa, de 16 de julho de 2019, que trata da comissão e reuniões realizadas para a elaboração do Plano de Gestão de Riscos de TIC;

Os riscos institucionais e seus controles internos devem ser geridos de forma integrada, objetivando o estabelecimento de um ambiente de controle e gestão de riscos eficaz. A política de gestão de risco estabelece que esta tarefa deve ser desempenhada pelo Comitê de Riscos de Tecnologia da Informação e Comunicação (CRTIC) e pela Diretoria de Riscos de Tecnologia da Informação e Comunicação (DRTIC), os quais as denominações serão descritas nas próximas seções.

2.3. Diretoria de Riscos de Tecnologia da Informação e Comunicação – DRTIC

Os riscos institucionais e seus controles internos devem ser geridos de forma integrada, objetivando o estabelecimento de um ambiente de controle e gestão de riscos eficaz, tarefa a ser desempenhada pela DRTIC. Para a efetivação da gestão de riscos de TIC no âmbito do centro, ficam estabelecidas as responsabilidades dos diversos agentes envolvidos. A DRTIC possui como principal propósito elaborar e realizar a gestão do Plano de Gestão de Riscos de TIC.

São competências da DRTIC, governança e controles:

I. Promover práticas e princípios de conduta e padrões de comportamentos;
II. Institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;
III. Promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;
IV. Garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
V. Promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;
VI. Promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;
VII. Submeter para apreciação e aprovação do CGD, políticas, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
VIII. Supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;
IX. Liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no centro;

X. Estabelecer e definir o apetite a risco: limites de exposição a riscos globais do centro, bem com os limites de alçada ao nível de unidade, política pública, ou atividade;
XI. Estabelecer e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
XII. Emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos; e
XIII. Monitorar as recomendações e orientações deliberadas pelo Comitê, aprovadas pelo CGD.
XIV. Submeter para apreciação e aprovação do CGD propostas de políticas, diretrizes, objetivos e estratégias de TIC;
XV. Submeter para apreciação e aprovação do CGD os planos estratégicos e táticos e os indicadores de desempenho de TIC;
XVI. Submeter para apreciação e aprovação do CGD as demandas para provimento de novas soluções de TIC de natureza institucional, assim como demandas de manutenção com impacto significativo sobre os planos de TIC;
XVII. Acompanhar, periodicamente, a execução dos planos de riscos, estratégicos e táticos de TIC, a evolução dos indicadores de desempenho de TIC e outras informações relativas à gestão dos riscos e ao uso de TIC no CTIC / Unifesspa, de modo a reavaliar prioridades, identificar eventuais desvios e determinar correções necessárias;
XVIII. Analisar as medidas de transparência, comunicação e conformidade apreendidas pelo CGTIC;
XIX. Analisar outros assuntos inerentes à área de gestão de riscos de TIC, ainda que não especificados neste artigo, desde que determinados por autoridade competente.

2.4. Comitê de Riscos de Tecnologia da Informação e Comunicação - CRTIC

Para a efetivação da gestão de riscos de TIC no âmbito do centro, ficam estabelecidas as responsabilidades dos diversos agentes envolvidos. O CRTIC possui como principal propósito garantir a continuidade e aperfeiçoamento do Plano de Gestão de Riscos de TIC e da Política de Gestão de Riscos de TIC;

São competências do CRTIC:

I. Garantir a continuidade e aperfeiçoamento do Plano de Gestão de Riscos de TIC;
II. Garantir a continuidade e aperfeiçoamento da Política de Gestão de Riscos de TIC;
III. Analisar, avaliar, monitorar, no respectivo âmbito, os riscos mapeados, aplicar as medidas estabelecidas no Plano de Gestão de Riscos de TIC e identificar situações que envolvem risco;
IV. Fornecer orientações gerais e monitorar a política de risco de TIC a nível gerencial
V. Estabelecer objetivos e metas de risco para os diversos ativos e para a própria área de risco;
VI. Estabelecer parâmetros e métricas para a gestão de riscos sobre os ativos, controlando-as, solicitando relatórios e o desenvolvimento de sistemas;
VII. Avaliar resultados e performance da DRTIC, solicitando modificações e correções;
VIII. Orientar as diversas áreas da gestão de riscos de TIC, indicando riscos, solicitando revisões de
IX. Processo, metas e indicadores; evitando desenquadramentos, erros ou falhas ao gerir riscos de qualquer natureza ou impacto no centro;
X. Prestar reporte sobre decisões que gerem impactos no centro e no apetite a risco, quando solicitados pelo CGD.
XI. Oficializar e documentar decisões por meio de processo eletrônico / memorando, circulados a todos os membros da DRTIC.

O CRTIC, assim como o DRTIC e outras divisões/departamentos no que tange a governança e controles poderão ser apoiados por outras unidades interna e externas, como CGTIC/CTIC, SEPLAN, Autoria Interna (AUDIN), a qual prestará serviços de consultoria visando o aprimoramento da governança, do gerenciamento de riscos e dos controles da gestão, por meio da avaliação objetiva quanto à eficácia do gerenciamento de riscos; orientação quanto às suas etapas; disponibilização de ferramentas e técnicas utilizadas por ela na análise de riscos e controles; e proposição de recomendações quando necessário. Não são atividades atribuíveis à outras unidades internas e externas que poderão apoiar o CR, sem prejuízo de outras que ofereçam riscos à sua independência e objetividade:

I. estabelecer o apetite a risco ou risco aceitável;
II. tomar decisões sobre as respostas aos riscos;
III. implantar as respostas aos riscos em nome da administração; e
IV. responsabilizar-se pelo gerenciamento de riscos.

2.5. Comitê de Governança Digital – CGD

Para a efetivação da gestão de riscos de TIC no âmbito do centro, ficam estabelecidas as responsabilidades dos diversos agentes envolvidos. O papel do Comitê de Governança Digital (CGD) na gestão de riscos de TIC do CTIC / Unifesspa possui como principal propósito apreciar e aprovar o Plano de Gestão de Riscos de TIC, assim como a Política de Gestão de Riscos de TIC, e todas as demais decisões estratégicas no seu escopo de atuação relacionadas aos riscos de TIC.

São competências do CGD no escopo de Gestão de Riscos de TIC:

I. Aprovar, analisar, avaliar e acompanhar o Plano de Gestão de Riscos de TIC;
II. Aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
III. Aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
IV. Aprovar propostas de políticas, diretrizes, objetivos e estratégias de TIC;
V. Aprovar os planos estratégicos e táticos e os indicadores de desempenho de TIC;
VI. Aprovar as demandas para provimento de novas soluções de TIC de natureza institucional, assim como demandas de manutenção com impacto significativo sobre os planos de TIC;

3. Política de Gerenciamento de Riscos

A implantação e criação da Política de Gestão de Riscos de TIC do CTIC / Unifesspa considera a necessidade de estabelecer diretrizes norteadoras para o gerenciamento de riscos de TIC no centro, a necessidade de maior qualificação da gestão administrativa e acadêmica em todos os níveis, conforme estabelecido no Plano Diretor de TIC (PDTIC) e Plano de Desenvolvimento Institucional (PDI), assim como estabelece leis e instruções normativas citadas na seção de escopo legal no decorrer deste documento.

A Política de Gestão de Riscos do CTIC tem por objetivo assegurar aos gestores o acesso tempestivo às informações quanto aos riscos a que a instituição está exposta, melhorando o processo de tomada de decisão e ampliando a possibilidade do alcance dos objetivos estratégicos expressos no PDTIC, PDI e nos demais planejamentos estratégicos.

A Política de Gestão de Riscos do CTIC tem, na missão, na visão, nos objetivos e nos princípios institucionais estabelecidos no seu PDTIC, os elementos norteadores da sua implantação e execução.

Esta política aplica-se a todas os departamentos, coordenadorias e direções do CTIC, na gestão dos riscos que impactam no seu ambiente. Na implantação do Plano de Gerenciamento de Riscos de TIC e de suas sucessivas revisões, serão adotadas abordagens incrementais, com a definição gradativa dos objetivos e processos associados, até que todas as áreas e principais ativos estejam integrada à gestão de riscos de TIC.

São diretrizes desta política a gestão de riscos integrada ao planejamento estratégico estabelecido no PDTIC, levando em conta as políticas lá estabelecidas e os processos do centro; as classificações e níveis dos riscos conforme apresentadas no Plano de Gestão de Riscos de TIC utilizando abordagens qualitativas e quantitativas; a identificação e mapeamento dos riscos através dos processos; análise e avaliação dos riscos baseada na probabilidade e no impacto da sua ocorrência; a probabilidade de ocorrência será definida a partir de categorias, em função de suas especificidades e de sua complexidade; a matriz de Probabilidade X Impacto, cujo modelo é apresentado no Plano de Riscos de TIC do CTIC/Unifesspa correlaciona estes dois indicadores e baliza a estratégia de resposta aos riscos e o apetite ao risco do centro; o CTIC, a partir da sua matriz de Probabilidade X Impacto, definirá o tratamento e o monitoramento dos riscos.

Indicadores que permitam a análise do desempenho da gestão de riscos, tendo como base número de riscos previstos, números de riscos mapeados, número de riscos ocorridos, eficácia das medidas de tratamento e monitoramento adotadas, dentre outros deverão ser definidos para a retroalimentação e relatórios da gestão dos riscos.

Os responsáveis diretos por cada risco, com competência de implantar as medidas de tratamento e monitoramento, devendo reportar-se diretamente ao CR e DR devem ser definidos

seguindo as respectivas áreas de atuação documentadas no Plano de Gestão de Riscos de TIC do CTIC/Unifesspa.

Para suporte e capacitação da Gestão de Riscos de TIC do CTIC/Unifesspa políticas de capacitação institucional devem ser considerar formações específicas em gestão de riscos voltadas para todos os atores envolvidos, assim como treinamento e utilização de sistemas gerenciais como ferramentas de apoio a gestão de riscos do centro.

No prazo de 30 dias da aprovação desta política, o CTIC constituirá o Comitê de Riscos (CR) e a Diretoria de Riscos (DR), no prazo de até 180 dias de sua constituição, o comitê deverá elaborar, submeter à apreciação e aprovação do CGD e iniciar a implementação do Plano de Gestão de Riscos de TIC.

Esta política entra em vigor a partir da data de sua publicação, revogadas as disposições em contrário.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: Gestão de riscos - princípios e diretrizes, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31010: Gestão de riscos - técnicas para o processo de avaliação de riscos, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO GUIA 73:Gestão de riscos – Vocabulário, 2009.

BRASIL. MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. Governança de tecnologia da informação: artefato gestão de riscos de TIC / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Coordenação e Governança das Empresas Estatais, Coordenação-Geral de Gestão da Informação de Estatais; Universidade de Brasília – Brasília: MP, 2018. 21p