MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

COMITÊ DE GOVERNANÇA ESTRATÉGICO

RESOLUÇÃO DELIBERATIVA Nº 14 / 2025 - CGE (11.24.10.03)

Nº do Protocolo: 23077.168268/2025-16

Natal-RN, 17 de outubro de 2025.

Aprova a metodologia de riscos de segurança da informação da Universidade Federal do Rio Grande do Norte.

O VICE-PRESIDENTE DO COMITÊ DE GOVERNANÇA ESTRATÉGICO DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE, usando das competências previstas no artigo 16, §§ 1º e 3º, da Resolução 13/2022-CONSAD, de 14 de julho de 2022.

CONSIDERANDO o disposto no anexo da Resolução 013/2022-CONSAD, de 14 de julho de 2022, publicada no Diário Oficial da União em 27 de julho de 2022, no qual o CONSAD delega ao Comitê de Governança Estratégico a prerrogativa para aprovar e institucionalizar planos, modelos, políticas, diretrizes, metodologias, manuais, mecanismos de monitoramento, macroprocessos, processos e normas relacionadas às ações de governança da Universidade;

RESOLVE:

Art. 1º Aprovar a metodologia de riscos de segurança da informação da Universidade Federal do Rio Grande do Norte, anexo a essa resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

(Assinado digitalmente em 21/10/2025 09h15)
HENIO FERREIRA DE MIRANDA
VICE-PRESIDENTE
UFRN (11.00)
Matrícula: 347496

METODOLOGIA DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

1. INTRODUÇÃO

Este documento fornece diretrizes para a gestão de riscos de segurança da informação na UFRN. Essa metodologia tem por fundamento o Modelo de Gestão de Riscos Operacionais da UFRN (Resolução nº 1/2021 - CGRC/UFRN, de 27 de maio de 2021).

2. REFERÊNCIAS NORMATIVAS

- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.
- Lei nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, por meio do capítulo VII - da Governança, da Gestão de Riscos, do Controle e da Auditoria
- Resolução nº 13 - UFRN/CONSAD, de 14 de julho de 2022, que Institui o Sistema de Governança da Universidade Federal do Rio Grande do Norte - UFRN.
- Resolução nº 1/2021 - CGRC/UFRN de 27 de maio de 2021 que “Aprova o Modelo de Gestão de Riscos da Universidade Federal do Rio Grande do Norte - UFRN”.
- Norma Técnica ABNT NBR ISO/IEC 27005:2023 - Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação
- Norma Técnica ABNT NBR ISO 31000:2018 - Gestão de riscos - Diretrizes.
- Norma Técnica ABNT NBR ISO/IEC 31010:2021 - Gestão de riscos - Técnicas para o processo de avaliação de riscos.
- Plano de gestão de risco da TJPB/DITECT.
- Portaria SEGECEX nº 9, de 18 de maio de 2017, que aprovou o Roteiro de Auditoria de Gestão de Riscos (TCU)
- Tribunal de Contas da União. Roteiro de Avaliação de Maturidade da Gestão de Riscos /Tribunal de Contas da União. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018. 164 p.
- DANTAS, José Alves; RODRIGUES, Fernanda Fernandes; MARCELINO, Gileno Fernandes; LUSTOSA, Paulo Roberto Barbosa. Custo-benefício do Controle: Proposta de um Método para Avaliação com Base no COSO. Revista de Contabilidade, Gestão e Governança. 2010.

3. TERMOS E DEFINIÇÕES

- **Ameaça:** causa potencial de um incidente de segurança da informação que pode resultar em danos a um sistema ou prejuízos a uma organização.
- **Apetite pelo risco:** quantidade e tipo de riscos que uma organização está preparada para buscar ou reter.
- **Ativo:** qualquer bem, tangível ou intangível, que tenha valor para a Instituição.
- A**tivo de informação**: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.
- **Controle:** procedimentos e métodos estabelecidos para garantir que os riscos identificados não prejudiquem os objetivos organizacionais. Exemplos de controles são: normas, treinamentos, monitoramentos, auditorias, barreiras físicas etc.
- **Evento:** ocorrência proveniente de fontes internas ou externas a uma organização, que pode afetar a consecução dos objetivos.
- **Gestão de riscos:** atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.
- **Gestor de Risco:** Pessoa responsável pela gestão do risco de um ativo ou conjunto de ativos.
- **Impacto**: mede o potencial comprometimento do objetivo ou resultado, dada a ocorrência de um risco
- **Nível de risco inerente (NRI) de um evento**: nível de risco antes da definição do seu tratamento, incluindo controles internos.
- **Probabilidade de Risco:** é a chance de um risco se concretizar. Esse atributo é representado por uma escala de valores, por exemplo, de muito baixo a muito alto.
- **Processo de gestão de riscos**: aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos.
- **Risco:** efeito da incerteza em alcançar um ou mais objetivos da Instituição.
- **Risco Inerente (RI):** nível de risco antes de quaisquer ações de mitigação de risco terem sido levadas em conta.
- **Risco residual (RR):** risco remanescente após terem sido levadas em consideração as ações de mitigação.
- **Vulnerabilidade:** fraqueza de um ativo ou controle que pode ser explorada e então levar a um evento com consequência negativa.

4. OBJETIVO

O processo de gestão de riscos de segurança da informação tem como objetivo integrar o processo de tomada de decisões, desde a concepção da política ou projeto até sua implementação nas entregas dos serviços de Tecnologia da Informação. Este documento apresenta uma abordagem para gerenciamento dos riscos relacionados à segurança da informação por meio de um conjunto de atividades e tarefas que permitam identificar e adotar as medidas de proteção necessárias para reduzir ou eliminar os riscos aos ativos de informação e dos sistemas tecnológicos, promovendo a continuidade das atividades acadêmicas e administrativas, e equilibrando os custos operacionais e financeiros envolvidos.

5. METODOLOGIA DO PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos consistirá das seguintes etapas:

1. Estabelecimento de Contexto
    a. Definição do contexto; e
    b. Identificação dos processos e atividades críticas sujeitas a vulnerabilidades.
2. Processo de Avaliação de Riscos
    a. Identificação de riscos;
    b. Análise dos riscos; e
    c. Avaliação de riscos.
3. Tratamento de Riscos
    a. Formulação e seleção de opções para tratamento do risco;
    b. Planejamento e implementação do tratamento do risco;
    c. Avaliação da eficácia do tratamento; e
    d. Decisão se o risco residual é aceitável e, caso não, tratá-lo.
4. Monitoramento dos Riscos e Análise Crítica de Resultados
    a. Garantia de que o tratamento dos riscos seja eficaz, eficiente e econômico;
    b. Obtenção de informações para melhorar avaliações futuras de risco;
    c. Análise e aprendizado com os incidentes ocorridos;
    d. Detecção de alterações no contexto interno e externo, incluindo alterações nos critérios de risco e os próprios riscos; e
    e. Identificação de riscos emergentes.
5. Comunicação e Consulta de Riscos

   a. Acordo a respeito do gerenciamento dos riscos mediante a troca e/ou compartilhamento de informações sobre os riscos com seus proprietários e outras partes interessadas;
   b. Identificação dos responsáveis pelos riscos de segurança da informação; e
   c. Aprovação pelos proprietários de risco do(s) plano(s) de tratamento de risco e decisão a respeito da aceitação de riscos residuais.
6. Registro e Relato da Gestão de Riscos
   a. Documentação obrigatória.

5.1 Estabelecimento de Contexto

Essa etapa visa determinar o objetivo da gestão de riscos. Por exemplo, suporte a um sistema de gestão de segurança da informação (SGSI), suporte a plano de continuidade de negócios, preparação para um plano de resposta a incidentes, entre outros.

Nessa primeira etapa serão definidos o ambiente no qual o trabalho será desenvolvido, o escopo e os critérios a serem considerados no processo de gestão de riscos. A equipe responsável pela gestão de riscos deve identificar e catalogar, com a ajuda dos respectivos responsáveis pelos serviços, todos os processos e atividades críticas sujeitas a vulnerabilidades para, nas etapas posteriores, elaborar o gerenciamento dos riscos.

Ao estabelecer o contexto deve-se levar em consideração parâmetros externos e internos. No ambiente interno a organização busca atender seus objetivos (visão, missão e valores), tendo em conta sua cultura organizacional, estratégias, políticas, normas, diretrizes e modelos adotados. Já externamente, seus objetivos baseiam-se, entre outros, em fatores financeiros, regulatórios, econômicos e na expectativa das partes interessadas externas.

5.2 Processo de Avaliação de Riscos

O processo de avaliação de riscos é composto pelos seguintes subprocessos: (i) identificação de riscos, (ii) análise de riscos e (iii) avaliação de riscos.

5.2.1 Identificação de Riscos

"O propósito da identificação de riscos é determinar o que possa causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer" (NBR 27001, 8.2.1)

Pré-requisitos para a identificação de riscos

- Identificação dos ativos/processos: Identificar cada ativo ou processo e o responsável por ele.
- Identificação das ameaças: identificar tanto as fontes das ameaças acidentais, quanto as intencionais, de dentro ou de fora da organização.
- Identificação dos controles existentes: Identificar e verificar se os controles existentes estão funcionais.
- Identificação das vulnerabilidades: Identificar as vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização.
- Identificação das consequências: Identificar e registrar as consequências que as ameaças identificadas podem trazer aos ativos.

5.2.2 Análise de Riscos

Para cada um dos riscos identificados na etapa anterior, o gestor de risco deve avaliar a **probabilidade** do risco e o seu **impacto** para a UFRN. Com base nisso, poderá definir o nível desse risco. No caso de considerar o risco crítico, o gestor do risco deve fazer a indicação no sistema de gestão de riscos GERIFES.

A probabilidade de risco é a chance de um evento ocorrer, afetando o alcance de um determinado objetivo da instituição. Deve-se estimar essa probabilidade de acordo com uma escala qualitativa de cinco níveis, conforme demonstrado no Quadro 1.

Quadro 1 - Escala de Probabilidade de Ocorrência de Risco.

Nível	Descrição	Pontuação
Muito baixa	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.	1
Baixa	Há histórico de ocorrência, mas a frequência é baixa.	2
Média	Repete-se com frequência razoável ou há indícios que possam ocorrer nesse horizonte.	3

Alta	Repete-se com elevada frequência ou há muitos indícios que ocorrerão nesse horizonte.	4
Muito alta	Ocorrência quase garantida.	5

O impacto mede o potencial comprometimento do objetivo ou resultado, e deve ser estimado a partir da escala qualitativa definida no Quadro 2 a seguir.

Quadro 2 - Escala de Avaliação do Impacto de Ocorrência dos Eventos de Risco.

Nível	Descrição	Pontuação
Insignificante	Não afeta os objetivos.	1
Pequeno	Afeta pouco os objetivos.	2
Médio	Torna incerto ou duvidoso o alcance dos objetivos.	3
Grande	Torna difícil o alcance dos objetivos.	4
Crítico	Alta capacidade de impedir o alcance dos objetivos.	5

Baseados na definição de probabilidade e impacto da UFRN, conforme Quadros 1 e 2, é definido o Risco Inerente (RI) do evento a partir da matriz demonstrada no Quadro 3.

Quadro 3 - Representação Visual dos Limites de Cada Nível de Risco a Partir da Matriz de Riscos.

Nível de Risco Inerente		Probabilidade				
		Muito baixa 1	Baixa 2	Moderada 3	Alta 4	Muito Alta 5
Impacto	Crítico 5	5	10	15	20	25
	Grande 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Pequeno 2	2	4	6	8	10
	Insignificante 1	1	2	3	4	5

O Risco Inerente (RI) é dado pelo número inscrito em cada célula da matriz, obtido pela seguinte:

RI = PROBABILIDADE × IMPACTO

Quanto ao Nível de Risco Inerente (NRI), o Quadro 4, a seguir, ordena as possibilidades de NRI, desde o mais baixo, ao qual é atribuída pontuação de 1 a 2 (evento muito raro, de impacto muito baixo), até o mais elevado, ao qual é atribuída pontuação de 15 a 25 (probabilidade muito alta, evento praticamente certo e de impacto muito alto).

Quadro 4 - Pontuações e Respectivos Níveis de Riscos Inerentes (NRI).

Pontuação do RI	Nível do RI
15 a 25	Muito Alto
8 a 12	Alto
3 a 7	Médio
1 a 2	Baixo

O Quadro 3 e o Quadro 4 relacionam os valores do NRI e sua pontuação, sendo os níveis baixos em VERDE, os níveis médios em AMARELO, os níveis altos em LARANJA e os níveis muito altos em VERMELHO.

Dada a criticidade dos eventos em segurança da informação, o gestor do risco poderá optar por elevar o NRI, informando no sistema de apoio (Gerifes) que o ativo é considerado como crítico para a instituição, independente da classificação que tenha recebido na avaliação.

A análise de riscos só é completa quando são feitas as avaliações das ações adotadas para responder ao risco, obtendo-se o nível de risco residual. As formas de resposta a riscos podem variar entre reduzir, evitar, compartilhar ou aceitar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas pela gestão dos riscos sejam aplicadas eficazmente.

Para avaliar o efeito dos controles na mitigação de riscos, deve-se determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação dos controles, como descrito no Quadro 7 (TCU, 2017):

Quadro 5 - Escala para Avaliação de Controles.

Nível de Confiança (NC)	Avaliação do desenho e implementação dos controles (Atributos do controle)	Risco de Controle (RC)
Inexistente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1,0
Fraco NC = 20% (0,2)	Controles têm abordagens *ad hoc*, tendem a ser aplicados caso a caso. Aa responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Alto 0,8
Mediano NC = 40% (0,4)	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

Uma vez determinado o nível de confiança (NC), deve-se determinar o risco de controle (RC). O risco de controle pode ser entendido como a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente o alcance de objetivos. O RC é definido como complementar ao NC, conforme fórmula a seguir.

$$RC = 1 - NC$$

Após o estabelecimento do RC, é possível estimar o nível de risco residual (NRR), que é o risco que permanece após o efeito das respostas adotadas pela gestão, incluindo controles internos e outras ações, para reduzir a probabilidade e ou o impacto do evento. O propósito é demonstrar o efeito dos controles sobre os riscos inerentes (RI). Para isso, multiplica-se o nível de risco inerente (RI) pelo risco de controle (RC), utilizando a seguinte fórmula.

NRR = RI * RC

Caso o risco residual seja considerado alto, a gestão terá subsídios para demandar melhorias nas medidas de controle.

5.2.3 Avaliação dos Riscos

Considerando que o propósito da avaliação de riscos é apoiar decisões, deve-se comparar o nível de riscos com critérios de avaliação de riscos, particularmente critérios de aceitação de riscos para determinar se os riscos podem ou não ser aceitos. Isso deve ser feito analisando-se a probabilidade de ocorrência dos eventos e seu impacto (consequência para a organização), o grau de confiança na avaliação e o efeito cumulativo. Esta avaliação deve ocorrer, conforme a periodicidade definida a seguir no Quadro 6, ou a qualquer momento que se julgue necessário.

Quadro 6 - Periodicidade da Avaliação Segundo o Nível de Risco.

Nível de risco inerente	Periodicidade da avaliação
Muito alto	Trimestral
Alto	Semestral
Médio	Semestral
Baixo	Anual

O resultado da avaliação de riscos deve ser validado nos níveis apropriados da organização e devidamente registrado.

5.3 Tratamento de Riscos

O tratamento de riscos está relacionado à resposta a riscos encontrados. Envolve decidir se o risco vai ser tratado ou não, promovendo a priorização de tratamento. A estratégia de tratamento de risco adotada é composta pelas opções: mitigar o risco, aceitar o risco, evitar o risco e transferir o risco, conforme descrito a seguir.

- **Mitigar**: o risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles para que o risco residual possa ser reavaliado e considerado aceitável.
- **Aceitar**: o objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, tais como: risco de baixo nível ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco.
- **Evitar**: inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho.
- **Transferir**: redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.

5.4 Plano de Tratamento de Riscos

Definida a estratégia, será realizado o plano de tratamento de riscos que deve descrever claramente as ações que serão realizadas.

Os planos de tratamento de riscos devem estar integrados aos planos e processos de gestão da unidade.

O plano de tratamento deve incluir:

I - justificativa para seleção das opções de tratamento, incluindo os benefícios esperados a serem obtidos;

II - responsáveis por aprovar e executar o plano;

III - as ações propostas;

IV - os recursos requeridos, incluindo contingências; e

V - cronograma contendo os prazos que ações sejam iniciadas e concluídas.

5.5 Monitoramento dos Riscos e Análise Crítica de Resultados

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. O monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados devem ser uma parte planejada do processo de gestão de riscos.

Os gestores de riscos possuem o papel de monitorá-los e desenvolver os relatórios anuais das ocorrências dos riscos e da qualidade dos mecanismos de controle adotados.

5.5 Comunicação e Consulta

A comunicação visa assegurar que as informações sobre riscos sejam compartilhadas de forma clara, precisa e oportuna com as partes interessadas relevantes. A consulta de riscos tem como objetivo obter o feedback e a participação das partes interessadas para enriquecer a avaliação e o tratamento dos riscos.

A consulta é um processo bidirecional de comunicação, que consiste na disponibilização das informações consolidadas em local de fácil acesso aos interessados, como o portal da Governança da UFRN.

A função de reportar é de toda comunidade, caso perceba novos eventos de riscos, que podem impactar no processo e nos objetivos estratégicos da UFRN.

6. FERRAMENTA DE APOIO À GESTÃO DE RISCOS

Para dar apoio à gestão dos riscos de segurança da informação, será utilizado o sistema de Gestão de Riscos das IFES Gerifes (https://gerifes.ufrn.br/).

7. PAPÉIS E RESPONSABILIDADES

Para gerenciar o processo de gestão de riscos em segurança da informação na UFRN, ficam definidos os seguintes responsáveis:

I. Comitê de Governança Estratégico (CGE): responsável por revisar regularmente o desempenho do sistema de gestão de riscos, alinhando os riscos e as estratégias de maneira eficiente. Além de aprovar a metodologia da gestão de riscos em segurança

da informação e apoiar a inovação e a adoção de boas práticas de gestão de governança, de riscos, de controles internos e de integridade;

II. Comitê Gestor de Riscos e Controles Internos (CGRCI): responsável pela elaboração dos planos, políticas, diretrizes, metodologias, manuais e mecanismos de monitoramento e comunicação para gestão de riscos e controles internos. Deve implementar controles internos com foco em ações preventivas, estabelecer limites de exposição a riscos e determinar os níveis de tolerância e conformidade com os riscos. Também deve supervisionar o mapeamento e a avaliação dos riscos, além de liderar a institucionalização da gestão de riscos e controles internos, oferecendo suporte à sua implementação, além de emitir recomendações e orientações para aprimorar a gestão de riscos e controles internos.

III. Comitê Gestor de Segurança da Informação (CGSI): responsável por gerenciar os riscos cibernéticos e de segurança da informação, alinhando a proteção da informação com os objetivos estratégicos organizacionais, preparando a organização para proteger dados sensíveis e cumprir com obrigações regulatórias;

IV. Secretaria de Gestão de Projetos (SGP) e Secretaria de Governança Institucional (SGI): são responsáveis por assegurar que os riscos sejam gerenciados de maneira eficaz e que a organização esteja pronta para enfrentar imprevistos que possam afetar seus objetivos estratégicos; manter o sistema de gestão de riscos; e definir diretrizes de integração do processo de gestão de riscos aos processos organizacionais;

V. Superintendência de Tecnologia da Informação (STI): responsável, principalmente, pela proteção dos ativos de informação e na segurança dos sistemas de tecnologia, atuando no nível operacional, implementando as estratégias e políticas definidas pela alta gestão; e

VI. Gestor/proprietário de riscos: responsável por garantir que os riscos sejam adequadamente identificados, avaliados, monitorados e controlados, protegendo a organização contra perdas