UNILAB
Universidade da Integração Internacional da Lusofonia Afro-Brasileira

sgit | SECRETARIA DE GOVERNANÇA, INTEGRIDADE E TRANSPARÊNCIA

PLANO E METODOLOGIA DE GESTÃO DE RISCOS

sgit@unilab.edu.br

Sumário

Lista de Abreviaturas e Siglas

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CGU - Controladoria Geral da União

Conad - Conselho Administrativo

Consuni - Conselho Universitário

DTI - Diretoria de Tecnologia da Informação

IN - Instrução Normativa

INEP - Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira

ISO - *International Organization for Standardization*

KRI - Key Risk Indicators - Indicadores Chave de Risco

LAI - Lei de Acesso à Informação

LGPD - Lei Geral de Proteção de Dados

MEC - Ministério da Educação

MGI - Ministério da Gestão e da Inovação

PDI - Plano de Desenvolvimento Institucional

PGR - Plano de Gestão de Riscos

Proadi - Pró-Reitoria de Administração e Infraestrutura

Prograd - Pró-Reitoria de Graduação

Propae - Pró-Reitoria de Políticas Afirmativas e Estudantis

RB/RM/RA/RE - Risco Baixo/Médio/Alto/Extremo

RCSA - *Risk and Control Self-Assessment* - Autoavaliação de Riscos e Controles

SGIT - Secretaria de Governança, Integridade e Transparência

SIGAA - Sistema Integrado de Gestão de Atividades Acadêmicas

SIGRH - Sistema Integrado de Gestão de Recursos Humanos

SIPAC - Sistema Integrado de Patrimônio, Administração e Contratos

Sitai — Sistema de Integridade, Transparência e Acesso à Informação

SLA - Acordo de Nível de Serviço

TCU - Tribunal de Contas da União

UGI - Unidade de Gestão da Integridade

Unilab - Universidade da Integração Internacional da Lusofonia Afro-Brasileira

1. Introdução e Propósito

A gestão de riscos é componente estruturante da governança pública, pois fornece segurança razoável para o alcance dos objetivos institucionais — ensino, pesquisa, extensão, gestão e integridade — ao sistematizar como a Universidade identifica, avalia, trata, monitora e comunica os riscos que podem afetar esses objetivos. Na Unilab, a matéria foi normatizada pela Resolução CONAD/Unilab nº 20/2025, que institui a Política de Gestão de Riscos, determina sua observância por todas as unidades, outorga à SGIT a elaboração da minuta do Plano de Gestão de Riscos (PGR) e fixa requisitos como a definição do apetite ao risco e tolerâncias, além da implementação gradual. Esta Metodologia concretiza tais determinações, oferecendo critérios e procedimentos para a aplicação cotidiana da Política.

No plano federal, a Metodologia se alinha a três pilares normativos: (i) o Decreto nº 9.203/2017, que institui a Política de Governança e explicita a integração entre governança, gestão de riscos e controles internos, (ii) a Instrução Normativa Conjunta MP/CGU nº 01/2016, que disciplina a sistematização de práticas de gestão de riscos, controles internos e governança no Executivo Federal, e (iii) o Sistema de Integridade, Transparência e Acesso à Informação (Sitai), instituído pelo Decreto nº 11.529/2023, que integra integridade, transparência e acesso à informação e orienta a articulação institucional dos temas.

Desse modo, a presente Metodologia visa: (a) traduzir a Política da Unilab em procedimentos claros e proporcionais ao contexto institucional; (b) compatibilizar-se com o Referencial Técnico da Atividade de Gestão da Integridade aprovado pela Portaria Normativa CGU nº 234/2025; e (c) preservar coerência técnica com boas práticas nacionais (TCU/CGU/MGI).

2. Enquadramento institucional e governança

O arranjo institucional da Unilab distribui competências entre órgãos colegiados, alta administração e unidades especializadas. O Estatuto (art. 37, VII) atribui ao Conselho Administrativo (Conad) a competência para deliberar sobre governança, controles internos, gestão de riscos e integridade, conferindo legitimidade e capacidade decisória às deliberações sobre prioridades de risco, definição de apetite e tolerâncias, acompanhamento de indicadores e validação da matriz de riscos institucional.

Esse comando estatutário é operacionalizado pela Política de Gestão de Riscos, que: (i) institui a Política; (ii) determina que a SGIT elabore a minuta do PGR para apreciação do Conad, que exerce a função de Comitê Interno de Governança (art. 15-A do Decreto nº 9.203/2017); (iii) estabelece que o Plano conterá apetite e tolerâncias; e (iv) prevê implementação gradual em todas as áreas.

Em consonância com as boas práticas do setor público, a Política adota o Modelo das Três Linhas, delimitando papéis e fronteiras de atuação: 1ª linha — controles internos da gestão exercidos pelos responsáveis pelos macroprocessos acadêmicos e administrativos; 2ª linha — supervisão e monitoramento (SGIT, Conad e instâncias correlatas); e 3ª linha — Auditoria Interna, responsável por avaliação independente da efetividade dos controles e da supervisão.

Fonte: adaptado de THE INSTITUTE OF INTERNAL AUDITORS (IIA). The IIA's Three Lines Model, 2020.

No plano decisório, a Política explicita papéis-chave: ao Conad compete estabelecer a Política, aprovar o PGR, fixar tolerância e apetite; ao Reitor, estabelecer a estratégia e a estrutura de gerenciamento de riscos e dos controles internos da gestão; à SGIT, assessorar o Reitor, elaborar e gerir o PGR e orientar sua implementação; e à Alta Administração, garantir recursos e monitorar riscos.

A SGIT tem Regimento aprovado pelo Consuni (Resolução CONSUNI nº 166/2024), que a define como órgão de assessoramento direto à Reitoria, com autonomia técnica e operacional, acesso ao nível hierárquico superior e responsabilidade por propor ações e políticas em governança, integridade, gestão de riscos e transparência — exercendo, adicionalmente, a função de Unidade de Gestão da Integridade (UGI).

Quanto aos fluxos de informação e reporte, a Política determina que a avaliação seja representada em Matriz de Riscos e acompanhada por indicadores de risco e desempenho, avaliados periodicamente pelo Conad; as matrizes das unidades compõem a Matriz de Riscos Institucional, consolidada pela SGIT. A minuta do PGR e suas atualizações devem ser apresentadas periodicamente ao Conad.

3. Conceitos e definições

Risco. Possibilidade de ocorrência de um evento que afete adversamente os objetivos institucionais, mensurada pela combinação de probabilidade e impacto.

Gestão de riscos × Gerenciamento de riscos. *Gestão de riscos* é o conjunto estruturado e contínuo de processos, políticas e práticas adotados para identificar, avaliar, tratar, monitorar e comunicar riscos; *gerenciamento de riscos* é o processo de identificar, avaliar, administrar e controlar potenciais eventos, para fornecer segurança razoável quanto ao alcance de objetivos.

Apetite ao risco e tolerância. *Apetite* é o nível de risco que a Universidade se dispõe a assumir para atingir seus objetivos; *tolerância* é o limite operacional derivado desse apetite — usualmente materializado em KRIs com faixas Verde/Amarelo/Vermelho e gatilhos de escalonamento.

Controles internos. Medidas preventivas, detetivas e de atenuação/recuperação para reduzir probabilidade e/ou mitigar impacto.

Risco inerente e residual. *Inerente* é estimado antes de considerar controles; *residual*, após considerar a eficácia dos controles.

Registro de riscos, plano de tratamento e heatmap. O *registro de riscos* consolida evento, causas, consequências, controles, níveis inerente e residual, plano de tratamento, KRIs e responsável; o *plano* detalha ações, prazos, recursos e efeitos esperados; o *heatmap* é a visualização agregada na matriz 5×5 usada para priorização e acompanhamento.

4. Escopo e categorias de risco

O escopo da gestão de riscos abrange os processos acadêmicos e administrativos da Universidade, os projetos estratégicos (inclusive obras e aquisições relevantes), os contratos e parcerias com terceiros, os sistemas de informação e a gestão de dados, bem como as atividades de integridade e transparência. Para dotar o processo de uma linguagem comum, a Unilab adota a taxonomia oficial instituída pela Política de Gestão de Riscos: riscos estratégicos, financeiros/orçamentários, operacionais, legais/conformidade, imagem/reputação e integridade. Essa classificação é abrangente e não excludente: um mesmo evento pode tocar mais de uma dimensão; por isso, a regra metodológica é classificar pelo maior impacto, sem perder de vista os efeitos colaterais nas demais categorias.

A categoria "integridade" merece detalhamento: ela inclui eventos relacionados a corrupção, fraudes, irregularidades e desvios éticos e de conduta; seu desdobramento em subcategorias consta no Anexo da Resolução CONAD nº 20/2025 e deve ser atualizado periodicamente pelo Conad, a partir da evolução da maturidade institucional. Entre as subcategorias, destacam-se: conduta profissional inadequada; ameaças à imparcialidade/autonomia técnica; uso indevido de autoridade; nepotismo; conflitos de interesse; recebimento indevido de presentes/vantagens; gestão indevida de dados/informações e restrição indevida de publicidade/acesso. A SGIT, como unidade responsável por consolidar a Matriz de Riscos Institucional, deve propor ao Conad a manutenção ou atualização dessas subcategorias, com base em incidentes, auditorias, autoavaliações e no Referencial Técnico da Integridade (Portaria CGU nº 234/2025).

No contexto universitário, recomenda-se detalhar a taxonomia com "lentes setoriais" para facilitar oficinas (RCSA) e registros:

- **Acadêmico** (vinculado a "estratégico" e "operacional"): evasão, atraso de calendário, avaliação MEC/INEP/CAPES, integridade acadêmica;
- **Pesquisa e inovação** (operacional/legais): ética em pesquisa, propriedade intelectual;
- **Assistência estudantil** (operacional/financeiro): programas de permanência, alimentação, moradia;

- **TI e dados** (operacional/legais/reputação/integridade): disponibilidade de SIGAA/SIPAC/SIGRH; incidentes de LGPD; segurança cibernética;
- **Contratações e terceiros** (operacional/financeiro/integridade): planejamento, execução contratual, SLAs e continuidade;
- **Obras e patrimônio** (operacional/financeiro/integridade): prazos, custos, qualidade e transparência.

Essa vista matricial (categorias × áreas) permite mapear riscos críticos por macroprocesso, mantida a classificação oficial para efeito de comparabilidade institucional e reporte ao Conad.

5. Princípios metodológicos e referências

A Metodologia de Gestão de Riscos da Unilab observa, como diretriz central, os princípios estabelecidos na Política Institucional. Esses princípios são o fio condutor do "como" implementar, monitorar e aprimorar a gestão de riscos, em harmonia com o arcabouço federal — Decreto nº 9.203/2017, IN Conjunta MP/CGU nº 01/2016, Referencial do TCU (2018), Guia do MGI (2025) e ISO 31000:2018, além da Portaria CGU nº 234/2025 (Referencial Técnico da Integridade) e da Resolução CONAD/Unilab nº 20/2025.

I — Feita sob medida, alinhada ao contexto interno e ao perfil do risco.

II — Agregar valor e proteger o ambiente interno da Unilab.

III — Parte integrante dos processos organizacionais, de forma sistemática, estruturada e oportuna.

IV — Baseada nas melhores informações disponíveis.

V — Subsidiar a tomada de decisão e o planejamento estratégico.

VI — Apoiar a melhoria contínua dos processos organizacionais.

VII — Aprimorar a governança, a conformidade e a auditoria interna.

VIII — Promover transparência, inclusão, integridade e efetividade nas ações institucionais.

IX — Integrada às oportunidades e à inovação.

X — Considerar fatores humanos e culturais.

Do ponto de vista metodológico, a Unilab harmoniza essas diretrizes com as referências técnicas: adota o processo da ISO 31000 (contexto → identificação → análise →

avaliação → tratamento → monitoramento/comunicação); utiliza a Matriz 5×5 com as faixas RB/RM/RA/RE da Metodologia de Gestão de Riscos da CGU (2ª versão) e observa a documentação e proporcionalidade sugeridas pelo TCU.

6. Processo de gestão de riscos

A gestão de riscos da Unilab é concebida como um processo contínuo e cíclico que começa na compreensão do contexto e na definição de critérios, passa pela identificação, análise, avaliação e tratamento dos riscos e se consolida no monitoramento, comunicação e reporte. Esse encadeamento guarda conformidade com a Política de Gestão de Riscos aprovada pelo Conad, que determina a representação dos riscos por matriz (probabilidade × impacto), a adoção de respostas para mitigação e a seleção de indicadores para monitoramento; também estabelece que a Matriz Institucional é consolidada pela SGIT a partir das matrizes das unidades e acompanhada periodicamente pelo Conad.

6.1. Estabelecimento de contexto, escopo e critérios

O processo inicia pela definição do escopo (processo, projeto ou unidade), pela explicitação dos objetivos (PDI, metas e entregas), pelo mapeamento de partes interessadas, restrições e dependências críticas (pessoas, tecnologia, orçamento) e, de modo particularmente relevante, pela seleção dos critérios de análise (escalas de probabilidade e impacto). A Política estrutura esses elementos e determina que o detalhamento conste do Plano de Gestão de Riscos (com apetite e tolerâncias), cuja execução é gradual e com revisões em caso de realinhamento estratégico ou mudança significativa do risco.

Estabelecer critérios antes da identificação reduz vieses, padroniza julgamentos e assegura comparabilidade entre unidades — premissa consagrada pelo TCU e coerente com a ISO 31000. A Metodologia de Gestão de Riscos da CGU também parte de critérios explícitos para o cálculo do nível de risco (P×I) e para a classificação por faixas (RB/RM/RA/RE).

Exemplo prático. Em um processo acadêmico (p.ex., abertura de turmas), a probabilidade pode ser ancorada na frequência histórica de cancelamentos e o impacto na gravidade para o calendário e para a permanência estudantil. Com os critérios definidos, unidades distintas julgarão de forma consistente situações semelhantes.

6.2. Identificação de riscos

A identificação descreve cada risco no formato causas–evento–consequências e pode valer-se de oficinas RCSA, análise de incidentes, constatações de auditorias, mudanças organizacionais, riscos de terceiros e *horizon scanning*. Para riscos complexos, recomenda-se o diagrama *bow-tie*, que explicita barreiras preventivas (entre causas e evento) e barreiras de atenuação/recuperação (entre evento e consequências). A saída desta etapa é o Registro de Riscos, contendo, no mínimo, evento (causa-risco-consequência), controles existentes e sua eficácia, P/I inerentes e residuais, criticidade (P×I), situação versus apetite/tolerâncias, KRIs e plano de tratamento quando aplicável.

Exemplo prático (TI). Risco de indisponibilidade do SIGAA durante matrícula:

Causas — capacidade de banco insuficiente; mudança sem *stress test*.

Controles preventivos — *capacity planning*; janelas de mudança.

Controles detetivos — monitoramento de latência/erros.

Atenuação/recuperação — *rollback*; contingência de horários.

6.3. Análise de riscos (inerente e residual)

Para cada risco, estima-se Probabilidade (P) e Impacto (I) inerentes (sem controles) e, após a avaliação do desenho e da eficácia dos controles (preventivos, detetivos, corretivos), reestima-se P e I residuais. Na Unilab, adota-se a Matriz 5×5 e a classificação RB (0–4,99) / RM (5–11,99) / RA (12–19,99) / RE (20–25) — aplicáveis a inerente e residual — conforme a Metodologia de Gestão de Riscos da CGU, em aderência às boas práticas do setor público.

6.4. Avaliação e priorização

A criticidade é dada por P×I (1–25). A priorização considera: (i) nível residual versus Apetite/Tolerâncias; (ii) urgência e magnitude do impacto (p.ex., integridade/LAI/LGPD); e (iii) o custo–benefício das alternativas. A Metodologia de Gestão de Riscos da CGU padroniza o limite de exposição entre RA e RE; níveis residuais acima desse limite exigem plano de tratamento e, se necessário, escalonamento. A Política determina que a avaliação seja representada por Matriz de Riscos, com respostas e indicadores definidos, e que as Matrizes das Unidades componham a Matriz Institucional, consolidada pela SGIT e acompanhada pelo Conad.

6.5. Tratamento de riscos

As estratégias de tratamento compreendem: evitar, reduzir (mitigar), compartilhar/transferir (p.ex., seguros, cláusulas contratuais) ou aceitar (com justificativa e aprovação no nível competente). Cada plano deve especificar ações, responsáveis, prazos, custos, marcos, dependências e o efeito esperado no nível de risco/resiliência.

Exemplo prático (contratações). Para risco alto de inadimplemento de fornecedor crítico, combinar: multas, garantias, plano de continuidade do terceiro e monitoramento de desempenho.

6.6. Monitoramento, comunicação e reporte

Riscos Altos/Extremos devem ter KRIs com faixas Verde/Amarelo/Vermelho, fonte e frequência, acompanhando-se tendências e efetividade de planos/controles. A Política prevê indicadores avaliados periodicamente pelo Conad, consolidados pela SGIT a partir das matrizes das unidades; o processo é contínuo e sujeito a revisão quando houver realinhamento estratégico ou mudança significativa do risco.

6.7. Incidentes e melhoria contínua

Incidentes relevantes exigem registro, classificação de severidade e análise de causa-raiz, com ajustes em controles e KRIs. A aprendizagem institucional retroalimenta metas e critérios. A Política prevê capacitação contínua e a atualização periódica do Anexo “Riscos para Integridade” — por proposta da SGIT ao Conad — refletindo a maturidade da Universidade.

7. Critérios e escalas

A adoção de critérios claros e escalas padronizadas é condição para que diferentes unidades julguem riscos de modo consistente e comparável. Esta metodologia emprega uma escala 5×5 de Probabilidade e Impacto, combinada por meio da Matriz de Riscos, tanto para o risco inerente (antes dos controles) quanto para o residual (após os controles). O uso de matriz é exigência da Política de Gestão de Riscos da Unilab e deve vir acompanhado de

respostas e indicadores para monitoramento, com consolidação institucional pela SGIT e avaliação periódica pelo Conad.

Figura 1 - Matriz de Probabilidade x Impacto

IMPACTO	Muito Alto 5	5 RM	10 RM	15 RA	20 RE	25 RE
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
		PROBABILIDADE				

Fonte: Metodologia de Gestão de Riscos da CGU (2ª versão)

Nota. A escolha da matriz 5×5 e das faixas (RB/RM/RA/RE) segue a Metodologia de Gestão de Riscos da CGU e a Metodologia de Gestão de Riscos do MGI (modelos adotados como referência na Unilab) e harmoniza com o Referencial do TCU e com a ISO 31000, preservando comparabilidade e facilitando priorização.

7.1 Probabilidade (escala 1–5)

A Probabilidade representa a chance de ocorrência do evento de risco num horizonte compatível com o processo/objetivo analisado. Adota-se uma escala qualitativa-quantitativa com âncoras temporais; a calibragem abaixo é institucional e deve ser mantida para garantir comparabilidade:

- **1 – Raro**: evento muito incomum, esperado > 10 anos;
- **2 – Improvável**: pode ocorrer a cada 5–10 anos;
- **3 – Possível**: pode ocorrer a cada 1–5 anos;
- **4 – Provável**: tende a ocorrer ao menos uma vez/ano;

- **5 – Quase certo**: ocorre múltiplas vezes ao ano.

O uso de âncoras temporais reduz vieses na estimativa e está alinhado ao TCU e às Metodologias de Gestão de Riscos da CGU e do MGI (que partem de critérios explícitos para cálculo do nível de risco).

7.2 Impacto (escala 1–5)

Impacto é a gravidade das consequências caso o evento ocorra. Avalia-se o maior impacto entre as dimensões materialmente relevantes para a Unilab (princípio do "pior caso plausível"), evitando subdimensionamento de riscos multifacetados:

- **Acadêmico** (p. ex., interrupção de calendário, prejuízo a avaliações MEC/INEP/CAPES);
- **Financeiro/Orçamentário** (perdas, glosas, compromissos não honrados);
- **Operacional/Continuidade** (p. ex., indisponibilidade de SIGAA/SIPAC/SIGRH);
- **Legal/Conformidade** (descumprimento de prazos e sanções);
- **Reputação/Imagem** (repercussão pública);
- **Integridade/Conduta** (fraudes, corrupção, conflitos de interesse, uso indevido de dados).

Para fins desta Metodologia, o Impacto será classificado da seguinte forma:

1 – Muito baixo: efeitos localizados, rapidamente reversíveis, sem prejuízo relevante a metas, usuários ou conformidade;

2 – Baixo: prejuízo limitado, com correção simples e impacto restrito à unidade;

3 – Médio: prejuízo relevante, com atraso ou retrabalho significativo, podendo afetar entregas, usuários ou metas;

4 – Alto: comprometimento expressivo de processo, serviço, obrigação regulatória ou imagem, exigindo atuação prioritária da gestão;

5 – Muito alto: comprometimento grave ou prolongado dos objetivos institucionais, com repercussão acadêmica, regulatória, financeira, reputacional ou de integridade.

As dimensões de impacto acima dialogam com as categorias de risco previstas na Política da Unilab (que inclui, entre outras, riscos estratégicos, financeiros, operacionais, legais e de integridade; e traz anexo específico para riscos de integridade) e foram operacionalizadas nesta metodologia para orientar a medição do Impacto. A regra de "usar o

maior impacto" é prática recomendada em gestão de riscos públicos e coaduna com os modelos da CGU e do MGI.

Exemplo (TI): Se uma falha no SIGAA durante matrícula gera indisponibilidade de 3–4 horas e ampla repercussão local, considera-se Operacional/Continuidade (3 ou 4) e Reputação (3), registrando o maior valor na escala de Impacto.

7.3 Matriz 5×5 e faixas

A Matriz 5×5 resulta da combinação de Impacto (linhas) e Probabilidade (colunas). A classificação adotada utiliza como referência os modelos da CGU e do MGI:

- **RB – Risco Baixo: 0–4,99**
- **RM – Risco Médio: 5–11,99**
- **RA – Risco Alto: 12–19,99**
- **RE – Risco Extremo: 20–25**

A mesma matriz é aplicada ao risco inerente e ao residual, tornando explícito o efeito dos controles (diferença entre os níveis). A Política da Unilab determina que a avaliação de riscos seja representada por matriz (P×I), com respostas e indicadores definidos para o monitoramento. Esta abordagem é coerente com as diretrizes do TCU e com o arcabouço normativo federal de riscos/controles (IN Conjunta MP/CGU nº 01/2016).

7.4 Regra de ação

A regra de ação vincula a classificação à resposta e ao nível decisório, assegurando foco naquilo que mais ameaça a missão (produto P×I e apetite/tolerâncias).

- **RE / RA (Extremo/Alto)**: tratar imediatamente; reporte ao Conad; a aceitação de risco residual acima do apetite dependerá de justificativa da unidade, manifestação técnica da SGIT e deliberação do Conad.
- **RM (Médio)**: tratar por custo–benefício, com prazos definidos e monitoramento gerencial.
- **RB (Baixo)**: aceitar/monitorar (incluir em rotinas e revisões periódicas).

Os modelos da CGU e do MGI padronizam o limite de exposição entre RA e RE; riscos residuais acima desse limite exigem plano de tratamento e, quando necessário,

escalonamento (compatível com a exigência da Política de representar, responder e monitorar por indicadores).

8. Apetite a risco e tolerâncias

O apetite a risco expressa o nível de risco que a Universidade está disposta a assumir para cumprir seus objetivos; as tolerâncias traduzem esse apetite em limites operacionais mensuráveis para gestão e monitoramento. Na Unilab, a instância competente para definir o apetite e estabelecer o nível de tolerância é o Conad, tendo por base os objetivos do PDI e a análise do ambiente interno e externo. Essa orientação deve constar do Plano de Gestão de Riscos, instrumento que também detalha os processos e orienta a implementação gradual em todas as áreas.

O apetite e as tolerâncias se desdobram em KRIs (Indicadores-chave de Risco) com faixas de controle (Verde/Amarelo/Vermelho), gatilhos de escalonamento e rotina de reporte. A Política prevê que tais indicadores sejam avaliados periodicamente pelo Conad, com consolidação técnica pela SGIT.

Princípios práticos

(a) Clareza: declarações qualitativas objetivas por categoria de risco; **(b) Mensuração**: KRIs com limites e periodicidade; **(c) Governança**: alçadas e prazos de resposta/escala; **(d) Integração**: diálogo com o Programa/Plano de Integridade; **(e) Revisão:** ajuste anual ou por mudança material de contexto.

8.1. Método de definição

Passo 1 — Conectar ao PDI e ao contexto: listar objetivos estratégicos e operacionais (acadêmicos, administrativos, TI, integridade), identificar restrições e dependências críticas e resumir riscos chave por categoria (estratégico, financeiro, operacional, legal/conformidade, reputação, integridade).

Passo 2 — Formular o apetite (declarações qualitativas): redigir, por categoria, o que a Unilab aceita ou não aceita. Exemplos: “tolerância zero a fraude/corrupção e a vazamento intencional de dados”; “propensão moderada à inovação pedagógica com salvaguardas”.

Passo 3 — Traduzir em tolerâncias (limites numéricos): escolher KRIs que reflitam a exposição e definir faixas (Verde/Amarelo/Vermelho) coerentes com a matriz 5×5 e com o histórico institucional.

Passo 4 — Definir gatilhos e alçadas: estabelecer gatilhos de atenção (Amarelo) e críticos (Vermelho), com prazos e responsáveis (p.ex., Amarelo: plano em 30 dias; Vermelho: comunicação imediata à SGIT e reporte ao Conad).

Passo 5 — Aprovar e comunicar: submeter a minuta ao Conad para aprovação; comunicar às unidades; registrar os KRIs no repositório institucional e publicar o anexo de apetite/tolerâncias no Plano de Gestão de Riscos.

8.2. Exemplos orientativos de apetite e tolerâncias

- **Integridade**: tolerância zero a fraude/corrupção, favorecimento e vazamento intencional de dados.

KRIs (exemplos): denúncias de integridade procedentes (nº e gravidade); conflitos de interesse declarados e geridos; tempo de resposta a apurações; incidentes de dados.

Gatilhos: *Amarelo:* aumento de tendência acima da média histórica → ação corretiva; *Vermelho:* caso grave/procedente ou incidente de dados com impacto relevante → escala imediata.

- **Operacional/TI (serviços críticos, p.ex., SIGAA/SIPAC/SIGRH)**: indisponibilidade não planejada dentro de limites mensais por serviço (p.ex., ≤ 2h/mês como referência inicial).

KRIs (exemplos): indisponibilidade total/ parcial; falhas críticas; vulnerabilidades críticas em aberto.

Gatilhos: *Amarelo*: tendência de indisponibilidade acima do limite por 2 ciclos; *Vermelho*: evento único acima do limite mensal ou vulnerabilidade crítica sem correção no prazo pactuado.

- **Legal/Conformidade**: próximo de 100% de prazos legais críticos cumpridos; 0 descumprimentos deliberados.

KRIs: % de prazos legais críticos cumpridos; nº de ações corretivas pendentes; atendimentos LAI no prazo; respostas a titulares (LGPD).

Gatilhos: *Amarelo*: queda abaixo de 98% em prazos críticos; *Vermelho:* sanção/auto de infração ou queda <95%.

- **Acadêmico/Assistencial**: assegurar continuidade do calendário e marcos de avaliação (MEC/INEP/CAPES) com tolerâncias definidas pela área; tolerância muito baixa a interrupções de semestre/estágios obrigatórios.

  KRIs: cancelamentos/turmas impactadas; *backlog* de estágios/defesas; atrasos em avaliações.

- **Financeiro/Orçamentário:** desvios não planejados dentro de teto pactuado no ciclo orçamentário; perdas operacionais dentro de patamar aceitável pelo risco-benefício das atividades.

  KRIs: % de execução; glosas; perdas operacionais; passivos contingentes.

Nota: a definição final dos números (limites por KRI) deve considerar maturidade dos controles, histórico de eventos e capacidade de resposta da(s) unidade(s). Para riscos residuais acima do limite de exposição (tipicamente entre "Alto" e "Extremo" na matriz 5×5), exige-se plano de tratamento e, se necessário, escalonamento.

8.3. Uso no dia a dia (monitorar, escalar, revisar)

Monitorar: acompanhar KRIs na frequência definida (mensal para riscos Extremos; bimestral/trimestral para Altos; semestral/anual para Moderados/Baixos), com tendências e análise de causa para desvios.

Escalar: ultrapassou Vermelho → notificação imediata ao dono do risco e à SGIT; reporte ao Conad no próximo ciclo (ou *ad hoc*, conforme gravidade); aceites fora do apetite devem ter justificativa e alçada definida.

Revisar: ao menos anualmente ou quando houver mudança material (normativa, tecnológica, orçamentária, acadêmica), submetendo ao Conad a atualização de apetite/tolerâncias e, se for o caso, os descritores de Probabilidade/Impacto.

8.4. Transparência e responsabilização

A SGIT (como unidade de governança, integridade e riscos) assessora a Reitoria e consolida as matrizes de risco e painéis de KRIs, assegurando que a Alta Administração disponha de informações tempestivas para decidir e prestar contas à comunidade. Essa função é reiterada no Regimento da SGIT, que lhe confere autonomia técnica, e na Política, que explicita papéis e responsabilidades na governança de riscos.

9. Plano de Gestão de Riscos da Unilab

O Plano de Gestão de Riscos (PGR) é o instrumento que organiza, em horizonte plurianual, como a gestão de riscos será introduzida e consolidada na Unilab. Ele traduz a Política de Gestão de Riscos em decisões concretas sobre o que será priorizado, quem faz o quê, em que ritmo e com quais entregas mínimas, conectando esta Metodologia ao PDI e ao planejamento estratégico da Universidade.

O presente PGR foi elaborado pela SGIT e será submetido ao Conad para aprovação e revisões periódicas, observando o Estatuto da Universidade e a Resolução Conad nº 20/2025.

9.1 Objetivos e horizonte do Plano

O PGR tem por finalidade:

- orientar a introdução e o amadurecimento da gestão de riscos em toda a Universidade, começando pelos processos e projetos mais críticos;
- garantir que a identificação, análise, avaliação, tratamento e monitoramento de riscos sigam critérios e escalas padronizadas definidos nesta Metodologia;
- apoiar a governança, a integridade, a transparência e os controles internos, fornecendo informações estruturadas para a tomada de decisão da Alta Administração e do Conad;
- estimular que a gestão de riscos seja incorporada ao planejamento, à execução e ao monitoramento de processos, projetos, programas e contratos.

O horizonte do PGR será bianual, com vigência de 24 (vinte e quatro) meses, contados da data de sua aprovação pelo Conad, observada a compatibilidade com o PDI vigente. Durante a vigência, o Plano será revisto anualmente para atualização de objetos,

prioridades, cronograma, pontos focais e parâmetros de apetite e tolerâncias, bem como poderá ser revisto extraordinariamente sempre que houver mudança relevante de contexto normativo, tecnológico, orçamentário, acadêmico ou organizacional.

9.2 Objetos e prioridades da gestão de riscos

Em cada ciclo, o PGR definirá quais objetos de gestão de riscos serão trabalhados. Entre eles, poderão ser selecionados:

- macroprocessos acadêmicos e administrativos (ensino, pesquisa, extensão, assistência estudantil, gestão de pessoas, orçamento e finanças, contratações, TI, obras, patrimônio, entre outros);
- projetos estratégicos e iniciativas do planejamento institucional;
- contratos e parcerias considerados críticos pela unidade responsável;
- temas transversais de integridade, transparência e proteção de dados pessoais.

Para o primeiro ciclo de implementação do PGR, ficam priorizados os seguintes objetos de gestão de riscos:

I – licitações (compras) e gestão de contratos, sob responsabilidade da Proadi;

II – governança de TI e segurança da informação, sob responsabilidade da DTI;

III – assistência estudantil e pagamento de bolsas, sob responsabilidade da Propae;

IV – gestão acadêmica crítica, compreendendo, entre outros, matrícula, registro acadêmico, expedição de diplomas e indicadores regulatórios, sob responsabilidade da Prograd, com apoio da unidade responsável pelos registros acadêmicos e expedição de diplomas.

A priorização dos objetos do primeiro ciclo considera: (a) relevância estratégica para o cumprimento do PDI e das prioridades institucionais; (b) materialidade acadêmica, social, operacional e orçamentária; e (c) criticidade, à luz de constatações de auditoria, riscos de integridade, dependência tecnológica, exposição regulatória e impacto potencial sobre a prestação de serviços à comunidade acadêmica.

A relação dos objetos priorizados, com indicação das unidades responsáveis pelos riscos e dos respectivos pontos focais, consta do Anexo I deste PGR, passível de atualização anual.

9.3 Ciclos e fases de implementação

No primeiro ciclo de implementação, cada objeto priorizado deverá percorrer as fases previstas neste item em prazo máximo de 180 (cento e oitenta) dias, contado da formalização de seu início pela SGIT em articulação com a unidade responsável.

Para fins de organização e acompanhamento, adota-se o seguinte cronograma de referência para cada objeto:

Fase 1 – Preparação e sensibilização (até 30 dias): designação do ponto focal da unidade; alinhamento de escopo; levantamento preliminar de processos, sistemas, contratos, bases de dados e requisitos normativos relacionados ao objeto.

Fase 2 – Mapeamento e avaliação de riscos (de 31 a 90 dias): realização de oficina(s) de identificação e análise de riscos; elaboração da versão inicial do Registro de Riscos; identificação de controles existentes; definição preliminar de riscos inerentes e residuais.

Fase 3 – Tratamento e validação (de 91 a 150 dias): validação interna da matriz de riscos pela unidade responsável; definição de respostas aos riscos; elaboração de plano de tratamento para riscos residuais acima do apetite ou em faixa de tolerância crítica; definição dos KRIs iniciais.

Fase 4 – Consolidação e início do monitoramento (de 151 a 180 dias): encaminhamento da versão consolidada do Registro de Riscos à SGIT; consolidação em bases comparáveis; início do acompanhamento dos KRIs; definição da rotina de reporte periódico.

Concluído o prazo de 180 (cento e oitenta) dias, os objetos priorizados ingressarão em rotina de monitoramento trimestral, com consolidação técnica pela SGIT e reporte periódico ao Conad, sem prejuízo da periodicidade específica de apuração dos KRIs definida no Anexo II.

Durante o segundo ano de vigência do PGR, a ênfase recairá sobre o monitoramento, a revisão dos planos de tratamento, a recalibração dos KRIs e a eventual inclusão de novos objetos, conforme deliberação do Conad.

A SGIT coordenará os ciclos, mas a condução das oficinas, dos registros e dos planos será sempre compartilhada com as unidades responsáveis pelos processos, projetos ou contratos.

9.4 Responsabilidades e entregas das unidades

Para cada objeto incluído no PGR, a unidade responsável deverá, com apoio da SGIT, produzir e manter atualizados, no mínimo, os seguintes instrumentos:

a) Registro de Riscos: documento que consolida, para o objeto, a descrição dos riscos (causas–evento–consequências), a categoria de risco, os controles existentes e sua avaliação, os níveis inerente e residual (P×I), a classificação por faixas (RB/RM/RA/RE), a situação frente ao apetite e às tolerâncias e a indicação do responsável ("dono do risco").

b) Plano de Tratamento de Riscos: obrigatório sempre que o nível residual estiver acima do limite de exposição aprovado pelo Conad. Deve apresentar as ações de tratamento ou melhoria de controles, o tipo de resposta (evitar, reduzir, compartilhar/transferir ou aceitar), os responsáveis, os prazos, os recursos necessários e o efeito esperado no nível de risco.

c) Indicadores de risco e desempenho: para riscos altos ou extremos, deverão ser definidos indicadores-chave de risco (KRIs) e, quando couber, indicadores de desempenho, com faixas Verde/Amarelo/Vermelho e gatilhos de escalonamento.

d) Relatório sintético anual: documento curto, encaminhado à SGIT, com a evolução dos principais riscos do objeto, a execução dos planos de tratamento e as principais lições aprendidas.

Para os fins do primeiro ciclo de implementação, cada unidade responsável deverá designar, por ato interno de sua chefia, ao menos 1 (um) servidor e respectivo suplente como ponto focal do objeto priorizado.

O ponto focal atuará como articulador técnico-operacional da gestão de riscos no âmbito do objeto sob sua responsabilidade, cabendo-lhe, entre outras atribuições: apoiar a realização das oficinas de riscos; organizar informações e evidências; acompanhar a atualização do Registro de Riscos; monitorar os KRIs definidos; articular a execução das ações de tratamento; e manter interlocução regular com a SGIT.

Para preservar a atualidade do PGR, a identificação nominal dos pontos focais poderá constar de ato interno próprio da unidade com a indicação por cargo/função.

9.5 Monitoramento, reporte e revisão do PGR

Compete à SGIT:

- consolidar as matrizes de risco das unidades em uma Matriz de Riscos Institucional e em painéis de KRIs;
- acompanhar a execução dos planos de tratamento, prestando apoio metodológico e articulando interfaces com integridade, transparência e proteção de dados;
- elaborar relatórios periódicos ao Conad, destacando riscos mais críticos, tendências, incidentes relevantes e recomendações.

Compete ao Conad:

- aprovar o PGR e suas revisões;
- definir e revisar o apetite e as tolerâncias a risco da Unilab, por categoria e/ou tema, a partir de propostas da SGIT;
- acompanhar, em bases regulares, a evolução dos riscos estratégicos, operacionais e de integridade, bem como a efetividade dos planos de tratamento;
- deliberar sobre pedidos de aceitação de riscos acima do apetite, mediante justificativa da unidade e manifestação técnica da SGIT.

O PGR será revisado anualmente, ou a qualquer tempo por determinação do Conad, quando houver mudança relevante no contexto institucional ou nas diretrizes de governança.

9.6 Capacitação e comunicação

A SGIT, como unidade responsável por governança, integridade, gestão de riscos e transparência, coordenará, em articulação com as demais unidades:

- ações de capacitação contínua em gestão de riscos, integridade e controles internos, com foco em pontos focais, gestores de processos e membros da Alta Administração;
- iniciativas de comunicação interna (materiais explicativos, orientações, oficinas, divulgação de boas práticas e de lições aprendidas), com linguagem simples e exemplos ligados ao cotidiano da Unilab;
- integração entre o PGR, o Programa de Integridade, a agenda de transparência e a proteção de dados pessoais, de forma que os riscos de integridade e de tratamento

inadequado de dados sejam mapeados, registrados e tratados de maneira coordenada.

10. Considerações finais

A gestão de riscos na Unilab deve ser compreendida como um processo contínuo de apoio à decisão, e não como um fim em si mesma. Este Plano de Gestão de Riscos e esta Metodologia traduzem, em termos operacionais, a Política de Gestão de Riscos aprovada pelo Conad, em alinhamento com as referências federais sobre governança, riscos, integridade e controles internos.

A efetividade do modelo descrito dependerá do engajamento das unidades acadêmicas e administrativas, da atuação da Alta Administração e do acompanhamento sistemático pelo Conad e pela SGIT. Sua aplicação aos processos, projetos e temas priorizados no PGR deve ser vista como oportunidade de aprimorar controles, indicadores e formas de trabalho, a partir de incidentes, auditorias, avaliações externas e mudanças no contexto normativo, tecnológico, orçamentário e acadêmico. Por se tratarem de instrumentos dinâmicos, o Plano e a Metodologia deverão ser revisados periodicamente, cabendo à SGIT orientar sua compatibilização com eventuais normas setoriais específicas.

Por fim, o sucesso da gestão de riscos dependerá da consolidação de uma cultura em que a identificação de riscos e fragilidades não seja vista como punição, mas como instrumento de melhoria institucional e de prestação de contas à sociedade. A Unilab reafirma, assim, seu compromisso com a governança, a integridade, a transparência e a entrega de valor público por meio de uma gestão responsável de seus riscos.

11. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000:2018**. Gestão de riscos - Diretrizes. Rio de Janeiro: ABNT, 2018.

BRASIL. Controladoria-Geral da União. **Metodologia de Gestão de Riscos da CGU**. Versão 2.0. Brasília, DF: CGU, 2021.

BRASIL. Controladoria-Geral da União. **Portaria Normativa CGU nº 234, de 6 de novembro de 2025**. Aprova o Referencial Técnico da Atividade de Gestão da Integridade do Poder Executivo Federal. Brasília, DF: CGU, 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Guia de Gestão de Riscos do Ministério da Gestão e da Inovação em Serviços Públicos - MGI**. Brasília, DF: MGI, 2025.

BRASIL. Ministério do Planejamento, Orçamento e Gestão; CONTROLADORIA-GERAL DA UNIÃO. **Instrução Normativa Conjunta nº 1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, DF, 2016.

BRASIL. Presidência da República. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF, 2017.

BRASIL. Presidência da República. **Decreto nº 11.529, de 16 de maio de 2023**. Institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal. Brasília, DF, 2023.

BRASIL. Tribunal de Contas da União. **Referencial Básico de Gestão de Riscos**. Brasília, DF: TCU, 2018.

THE INSTITUTE OF INTERNAL AUDITORS. **The IIA's Three Lines Model: an update of the Three Lines of Defense**. Lake Mary, FL: The Institute of Internal Auditors, 2020.

UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA. **Resolução Complementar CONSUNI nº 3, de 4 de dezembro de 2020**. Aprova o texto definitivo do novo Estatuto da Universidade da Integração Internacional da Lusofonia Afro-Brasileira. Redenção, CE: Unilab, 2020.

UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA. **Resolução CONSUNI/UNILAB nº 166, de 22 de outubro de 2024**. Regimento Interno da Secretaria de Governança, Integridade e Transparência da Unilab. Redenção, CE: Unilab, 2024.

UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA. **Resolução CONAD/UNILAB nº 20, de 8 de outubro de 2025**. Aprova a Política de Gestão de Riscos da Universidade da Integração Internacional da Lusofonia Afro-Brasileira - Unilab. Redenção, CE: Unilab, 2025.

ANEXO I – OBJETOS PRIORITÁRIOS DO PRIMEIRO CICLO E UNIDADES RESPONSÁVEIS

Objeto priorizado	Unidade responsável	Prazo do primeiro ciclo
Licitações (compras), gestão de contratos; e Gestão acadêmica crítica: registro e expedição de diplomas	Proadi	Até 180 dias
Infraestrutura e segurança da informação de sistemas de TIC	DTI	Até 180 dias
Assistência estudantil e pagamento de bolsas	Propae	Até 180 dias
Gestão acadêmica crítica (seleção, matrícula, controle acadêmico) e indicadores regulatórios	Prograd	Até 180 dias

As unidades responsáveis poderão envolver unidades de apoio técnico, administrativo ou finalístico, sempre que a natureza do objeto priorizado assim exigir, sem prejuízo da responsabilidade principal da unidade indicada neste Anexo.

ANEXO II – APETITE, TOLERÂNCIAS E KRIs INICIAIS DO PRIMEIRO CICLO

Os parâmetros deste Anexo têm caráter inicial e orientativo, devendo ser revisados no primeiro processo anual de revisão do PGR, com base na disponibilidade, qualidade e estabilidade dos dados produzidos pelas unidades responsáveis.

Para fins deste Anexo:

- **Faixa Verde:** situação compatível com o apetite a risco definido;
- **Faixa Amarela:** situação fora do apetite ideal, porém ainda dentro da tolerância operacional, exigindo análise e ação corretiva em até 30 dias;
- **Faixa Vermelha:** situação acima da tolerância admitida, exigindo comunicação imediata à SGIT e tratamento prioritário, com reporte ao Conad.

Objeto priorizado	Declaração inicial de apetite a risco	KRI inicial	Faixa Verde	Faixa Amarela	Faixa Vermelha	Periodicidade
Licitações (compras) e gestão de contratos	Apetite baixo para atrasos operacionais e desconformidades formais; apetite muito baixo para falhas de fiscalização contratual; tolerância zero para fraude, favorecimento ou irregularidade grave.	Percentual de contratos vigentes sem fiscal formalmente designado	0%	>0% até 2%	>2%	Trimestral
Licitações (compras) e gestão de contratos	Apetite baixo para atrasos operacionais e desconformidades formais; apetite muito baixo para falhas de fiscalização contratual; tolerância zero para fraude, favorecimento ou irregularidade grave.	Percentual de processos prioritários de contratação concluídos fora do prazo planejado	até 10%	>10% até 20%	>20%	Trimestral

Objeto priorizado	Declaração inicial de apetite a risco	KRI inicial	Faixa Verde	Faixa Amarela	Faixa Vermelha	Periodicidade
Infraestrutura e segurança da informação de sistemas de TIC	Apetite baixo para indisponibilidade de serviços críticos; apetite muito baixo para vulnerabilidades críticas não tratadas no prazo e incidentes relevantes de segurança da informação.	Horas de indisponibilidade não planejada de sistemas críticos por mês	até 2 horas/mês	>2 até 4 horas/mês	>4 horas/mês	Mensal
Infraestrutura e segurança da informação de sistemas de TIC	Apetite baixo para indisponibilidade de serviços críticos; apetite muito baixo para vulnerabilidades críticas não tratadas no prazo e incidentes relevantes de segurança da informação.	Percentual de vulnerabilidades críticas sem tratamento no prazo pactuado	0%	>0% até 10%	>10%	Mensal
Assistência estudantil e pagamento de bolsas	Apetite muito baixo para atrasos ou interrupções de pagamento decorrentes de falha operacional; tolerância mínima para inconsistências que afetem a continuidade dos benefícios.	Percentual de pagamentos de bolsas realizados fora do calendário previsto	até 1%	>1% até 3%	>3%	Mensal

Objeto priorizado	Declaração inicial de apetite a risco	KRI inicial	Faixa Verde	Faixa Amarela	Faixa Vermelha	Periodicidade
Gestão acadêmica crítica	Apetite muito baixo para descumprimento de prazos críticos de seleção, matrícula, controle acadêmico, registro acadêmico, expedição de diplomas e obrigações regulatórias; tolerância mínima para atrasos com impacto acadêmico ou regulatório.	Percentual de prazos críticos da gestão acadêmica cumpridos no prazo	igual ou superior a 98%	igual ou superior a 95% e inferior a 98%	inferior a 95%	Trimestral

Para cada KRI constante deste Anexo, a unidade responsável deverá manter ficha técnica contendo, no mínimo, a definição do indicador, a fórmula de cálculo, a fonte do dado, a unidade responsável pela apuração e a periodicidade de coleta. Os KRIs poderão ser desdobrados em indicadores complementares pelas unidades responsáveis, desde que preservadas a comparabilidade institucional e a consolidação técnica pela SGIT.

Sempre que um KRI ingressar em Faixa Amarela, a unidade responsável deverá registrar análise sucinta da causa e definir medida corretiva ou preventiva em até 30 (trinta) dias; na hipótese de ingresso em Faixa Vermelha, deverá comunicar imediatamente a SGIT, revisar o respectivo Registro de Riscos e, quando cabível, apresentar plano de tratamento ao Conad. Os parâmetros deste Anexo poderão ser refinados após o primeiro ciclo de apuração, com base no histórico institucional, na capacidade de medição e na maturidade da gestão de riscos nas unidades.