PLANO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO (2026–2027)

UFRN | STI
Superintendência de Tecnologia da Informação

1. Introdução

Este Plano de Gestão de Riscos de Tecnologia da Informação (PGR-TI) da UFRN tem como objetivo orientar a aplicação da metodologia institucional de gestão de riscos, aprovada pela Resolução Deliberativa nº 01/2021 – CGRC, no contexto da gestão e responsabilidades da Superintendência de Tecnologia da Informação (STI).

A proposta não estabelece um processo de trabalho específico ou paralelo ao modelo de gestão de riscos da UFRN. Em vez disso, assegura que os riscos relacionados à TIC sejam devidamente identificados, classificados, tratados, monitorados e revisados, conforme a metodologia institucional, considerando as três esferas da atuação da área de TI: estratégica, tática e operacional.

---

2. Premissas e Referências

- O modelo de gestão de riscos adotado pela STI é o Modelo de Gestão de Riscos da UFRN, formalizado pela Resolução Deliberativa nº 01/2021 – CGRC e baseado nas normas ABNT NBR ISO 31000 e COSO/ERM.
- A gestão de riscos de TIC é parte integrante da gestão e governança de TIC da UFRN. A STI visa a implantação e amadurecimento dessa prática, com o objetivo de tornar sua gestão mais eficiente e melhorar a sua prestação de serviço. O monitoramento da evolução dessa prática está presente no plano estratégico de TI da UFRN (PDTIC 2024–2027), especificamente associado à meta M16 – Todos os riscos estratégicos, operacionais e de segurança da informação de grau alto ou muito alto monitorados.
- O plano reconhece a necessidade de priorização gradual, dado o estágio de maturidade atual da gestão de riscos na área de TIC.

---

3. Estruturas de Governança

A gestão de riscos de TIC na UFRN segue a estrutura institucional de governança de riscos aprovada pelo então Comitê de Governança, Riscos e Controles (CGRC). Dentro desse modelo, a execução da gestão de riscos de TIC envolve as seguintes instâncias e responsabilidades:

- **Secretaria de Gestão de Projetos (SGP):** responsável pelas etapas de Identificação, Análise e Definição do Tratamento dos Riscos, prestando suporte técnico à STI no registro e na estruturação dos eventos identificados, quando previsto no plano anual de gestão de riscos

- **Superintendência de Tecnologia da Informação (STI):** encarregada das fases de implementação dos controles de riscos, bem como acompanhamento e revisão dos riscos, assegurando a execução das ações de tratamento e acompanhamento contínuo.

- **Comitê Gestor de TIC (CGTIC):** delibera e revisa este plano antes do início de sua implementação, garantindo o alinhamento técnico e estratégico com o PDTIC e com a política de governança da UFRN.

- **Comitê de Governança Estratégico (CGE):** aprova o plano e acompanha sua execução, consolidando as ações de gestão de riscos da UFRN.

- **Secretaria de Governança Institucional (SGI):** responsável pelo monitoramento institucional dos riscos de TIC, assegurando a aderência do processo de gestão de riscos às diretrizes, políticas e metodologias de governança de riscos da UFRN.

---

4. Estruturas de Gestão de Riscos de TIC

Este plano estabelece uma abordagem focada na atuação sobre riscos **estratégicos e operacionais** relacionados à área de TIC da UFRN. Os riscos estratégicos correspondem àqueles associados ao cumprimento dos objetivos e **metas do PDTIC**, que representa o principal instrumento de planejamento estratégico da TIC na Universidade. Já os riscos operacionais abrangem os riscos vinculados ao sucesso das **práticas e processos de gestão de TIC**, bem como aos **ativos** de TI que os sustentam, como sistemas, infraestrutura, dados e serviços críticos. Essa estrutura permite uma visão integrada entre o direcionamento estratégico da TIC e sua operação cotidiana, fortalecendo o alinhamento entre governança, gestão e execução.

4.1 Riscos Estratégicos

Associados ao cumprimento dos objetivos estratégicos do PDTIC 2024–2027, traduzindo o direcionamento estratégico da área de TIC.

Exemplos:

- *M53 – 80% dos serviços de TI providos pela STI atendidos dentro da SLA.*
    - Risco: *Ausência de pessoal capacitado para atendimento em sistema e rede.*
    - Risco: *Ausência de documentação para consulta em sistema.*

4.2 Riscos Operacionais

Os riscos operacionais estão associados às práticas de gestão de TIC, conforme modelos amplamente reconhecidos como a ITIL v4, que estruturam processos essenciais para a entrega e sustentação dos serviços de tecnologia. Envolvem práticas como gestão de incidentes, problemas, mudanças, ativos, capacidade, continuidade e segurança da informação, entre outras que garantem a estabilidade e eficiência dos serviços prestados. Esses riscos também abrangem aspectos diretamente relacionados aos ativos de TI intrínsecos a essas práticas, como servidores, redes, bancos de dados, aplicações e equipamentos de infraestrutura, cuja disponibilidade e confiabilidade são fundamentais para a operação institucional da UFRN.
Exemplos:

1. Indisponibilidade de sistemas críticos (SIG-UFRN, SIGRH, SIPAC etc.);
2. Vazamento ou perda de dados sensíveis;
3. Falhas em backups, redundância ou segurança física do datacenter.

---

5. Metodologia

O modelo de gestão de riscos adotado pela UFRN estabelece uma metodologia estruturada para identificar, avaliar, tratar, monitorar e comunicar riscos que possam comprometer o alcance dos objetivos institucionais. Esse modelo é composto por dez etapas integradas, conhecidas como PROGERIS, que abrangem desde o estabelecimento dos objetivos e priorização de processos até o monitoramento e a comunicação dos riscos. A metodologia utiliza critérios qualitativos e quantitativos para avaliar a probabilidade e o impacto dos eventos de risco, permitindo classificá-los em níveis (baixo, médio, alto e muito alto) e priorizar o tratamento dos riscos mais críticos.

A abordagem também contempla o conceito de risco residual, que considera a eficácia dos controles existentes após a aplicação das medidas de mitigação. O processo é suportado pelo sistema GERIFES, que centraliza o registro, acompanhamento e validação dos riscos

institucionais. Mais detalhes sobre cada etapa, suas definições e tabelas de classificação podem ser consultados diretamente no Modelo de Gestão de Riscos da UFRN, documento original disponível na Secretaria de Governança Institucional (SGI) e referenciado neste plano como base metodológica oficial.

5.1. Papéis, Responsabilidades e Fluxos

A execução da gestão de riscos de TIC na UFRN envolve diferentes instâncias de governança, com papéis claramente definidos entre as áreas técnicas e estratégicas. As etapas de **identificação** e **classificação** dos riscos são conduzidas pela Secretaria de Gestão de Projetos **(SGP)**, enquanto a Superintendência de Tecnologia da Informação **(STI)** é responsável pela **implementação** dos controles, **acompanhamento** e **revisão** dos riscos. O Comitê Gestor de TIC **(CGTIC) delibera** sobre o plano e acompanha sua execução e o Comitê de Governança Estratégico **(CGE)** realiza a **aprovação** institucional. A Secretaria de Governança Institucional **(SGI)** é encarregada do monitoramento contínuo e sistemático dos riscos. Mais detalhes sobre as atribuições específicas, fluxos e ciclo de prestação de contas estão descritos no Anexo I – Estrutura de Papéis, Responsabilidades e Fluxos.

5.2. Priorização

Este plano estabelece que todos os riscos relevantes de TIC devem ser identificados e classificados conforme a metodologia institucional da UFRN. No entanto, reconhecendo as limitações de recursos e a necessidade de amadurecimento do processo, a prioridade inicial será o acompanhamento e monitoramento dos riscos classificados como de **grau alto e muito alto**. Essa escolha busca concentrar esforços na gestão dos riscos com maior potencial de impacto, assegurando uma **atuação eficaz e realista**. À medida que a maturidade em gestão de riscos evoluir e novas capacidades forem desenvolvidas, o escopo de acompanhamento e monitoramento **poderá ser ampliado** para abranger riscos de graus inferiores, de forma gradual e sustentável.

5.3. Estratégia de Implementação

A STI adotará uma abordagem progressiva e integrada, priorizando a consolidação da prática antes da ampliação do escopo. O processo seguirá as quatro etapas do modelo institucional:

1. **Identificação** dos riscos nas esferas operacionais e estratégicas;
2. **Classificação** dos riscos conforme probabilidade e impacto;

3. **Implementação** dos controles sobre os riscos;
4. **Acompanhamento** das ações de controle;
5. **Monitoramento** periódico dos riscos priorizados;
6. **Revisão** anual dos riscos e planos de tratamento.

---

6. Cronograma de Execução (2026–2027)

Trimestre	Atividades Principais	Resultado Esperado
1º Trim/2026	**Revisar** o inventário de riscos estratégicos a partir da nova versão do PDTIC e atualizar classificações.	Riscos estratégicos revisados.
2º Trim/2026	1. **Validar** com a SGP a revisão dos riscos estratégicos revisados 2. Iniciar o **acompanhamento** dos riscos estratégicos de grau alto e muito alto.	1. Riscos estratégicos validados. 2. Relatório de acompanhamento dos riscos estratégicos.
3º Trim/2026	**Revisar** e definir práticas e processos de gestão de TIC baseados na ITIL	Processos de gestão de TIC definidos e documentados
4º Trim/2026	**Revisar** e identificar novos riscos operacionais identificados e alinhar aos processos revisados.	Mapa de riscos operacionais definido
1º Trim/2027	1. **Compilar** resultados do plano e prestar contas 2. **Revisar** plano de gestão de riscos de TIC	1. Relatório do acompanhamento dos riscos estratégicos 2. Relatório da definição de riscos operacionais 3. Plano de gestão de riscos de TIC revisado
2º Trim/2027	Iniciar o **acompanhamento** dos riscos operacionais de grau alto e muito alto.	Relatório de acompanhamento dos riscos operacionais

3º Trim/2027	**Integrar** riscos estratégicos e operacionais em relatório consolidado.	Relatório integrado de riscos de TIC.
4º Trim/2027	Apresentar **resultados** ao CGTIC e CGRC e propor atualização do plano.	Plano de Gestão de Riscos de TIC 2028–2029 elaborado.

---

7. Acompanhamento

O acompanhamento dos riscos seguirá o processo institucional, com foco em riscos de grau alto e muito alto.

Proposta de indicadores:

- % de riscos estratégicos **acompanhados** dentro da periodicidade prevista;
- % de riscos **revisados** dentro do prazo anual;
- % de riscos com **grau reduzido** após implementação dos controles

Periodicidade proposta:

- Riscos estratégicos: acompanhamento **semestral**;
- Riscos operacionais: acompanhamento **semestral**.

Vale salientar que esta ainda é uma proposta inicial de acompanhamento, que deve ser revista à medida em que se consolide as listagens de riscos a serem acompanhados. Dada a maturidade atual do processo e conforme o cronograma apresentado, a STI ainda precisa revisar as listagens de riscos estratégicos e operacionais. Assim, este modelo de acompanhamento reflete uma visão ideal, que será revisada nas próximas versões do plano, quando houver inventário completo e atualizado dos riscos efetivamente gerenciados.

---

8. Capacitação

A capacitação dos gestores e servidores envolvidos na gestão de riscos de TIC deverá seguir o programa de **capacitação institucional** em gestão de riscos da UFRN, conduzido pela PROGESP/DDP. Não se justifica, neste momento, a criação de uma capacitação exclusiva para gestão de riscos de TIC, mas sim a integração do tema TIC nas capacitações gerais de gestão de riscos, abordando aspectos relacionados a ativos, processos e serviços tecnológicos. Além disso, recomenda-se a divulgação e incentivo à participação em cursos de referência oferecidos, tais como:

- ESR – Gestão de Riscos de Segurança da Informação e Privacidade (40h);
- ENAP – Introdução à Gestão de ‘Riscos (40h);
- ENAP – Gestão de Riscos em Projetos de Transformação Digital (10h).

---

9. Considerações Finais

A gestão de riscos de TIC é um componente essencial da governança de tecnologia da informação e comunicação da UFRN. Este plano reafirma o compromisso da STI em seguir o modelo institucional de gestão de riscos, fortalecer a cultura de riscos na área de TIC e garantir a integração entre a governança tecnológica e os objetivos estratégicos da Universidade.

Controle de Revisões do Documento

Versão	Data	Responsáveis	Observações
1.0	22 de out.…	Andre Dantas EURYANNE SILVA	Versão inicial a ser avaliada pela governança da UFRN. Versão revisada pela SGP.

Anexo I – Estrutura de Papéis, Responsabilidades e Fluxos

A gestão de riscos de TIC na UFRN é conduzida de forma integrada e participativa, envolvendo diferentes instâncias de governança, conforme descrito a seguir:

1. Estrutura Geral

O processo de gestão de riscos de TIC é estruturado com base no **Modelo de Gestão de Riscos da UFRN** (Resolução CGRC nº 01/2021), e conta com a atuação coordenada das seguintes unidades e instâncias:

Instância / Unidade	Papel principal	Responsabilidades	Fluxo de Atuação
Secretaria de Gestão de Projetos (SGP)	Técnica e metodológica	- Conduz as etapas **1 – Identificação** e **2 – Análise e Definição do Tratamento dos Riscos**. - Apoia as unidades na aplicação da metodologia institucional. - Mantém o sistema **GERIFES** atualizado e fornece suporte técnico..	Inicia o processo, promovendo oficinas e registrando riscos identificados em conjunto com a STI.
Superintendência de Tecnologia da Informação (STI)	Execução e coordenação operacional	- Conduz as etapas **4 – Acompanhamento** e **6 – Revisão dos riscos**. - Garante a **3 - Implementação** e execução dos planos de tratamento e a consolidação dos relatórios. - Presta contas ao CGTIC e CGE sobre a evolução da gestão de riscos de TIC.	Recebe da SGP os riscos identificados e classificados, implementa os controles e realiza o acompanhamento e revisões periódicas.

Comitê Gestor de TIC (CGTIC)	Instância técnica de deliberação	- Avalia e **revisa o Plano de Gestão de Riscos de TIC** antes de sua implementação. - Acompanha anualmente os resultados reportados pela STI. - Propõe ajustes e recomendações estratégicas.	Analisa e homologa o plano antes do envio ao CGE; acompanha sua execução.
Comitê de Governança Estratégico (CGE)	Instância de aprovação e supervisão	- **Aprova o Plano de Gestão de Riscos de TIC**. - Recebe relatórios anuais da STI e CGTIC. - Delibera sobre alinhamento com o plano institucional de governança.	Recebe o plano validado pelo CGTIC e acompanha os resultados anuais.
Secretaria de Governança Institucional (SGI)	Monitoramento dos riscos	- **Responsável pela etapa 5 - Monitoramento** - Verifica a aderência do processo de gestão de riscos de TIC às políticas, diretrizes e metodologias institucionais de governança e gestão de riscos.	Monitora os riscos ao longo do ciclo de gestão e analisa informações consolidadas pela STI e SGP.

---

2. Fluxo Resumido do Processo de Gestão de Riscos de TIC

1. Identificação, Análise e Definição do Tratamento dos Riscos (SGP)

→ Oficinas de levantamento de riscos nas três esferas (estratégica e operacional).
→ Registro dos riscos no sistema **GERIFES**.

2. Implementação de Controles, Acompanhamento e Revisão (STI)

→ Acompanhamento trimestral dos riscos estratégicos e táticos.
→ Elaboração de relatórios e planos de tratamento.

3. Monitoramento periódico dos riscos priorizados (SGI)

→ Monitoramento da evolução dos riscos e da efetividade dos controles adotados.
→ Análise de informações consolidadas pela STI e SGP.

4. Análise e Homologação (CGTIC)

→ Revisão técnica do plano e dos relatórios.

→ Emissão de parecer e validação para envio ao CGE.

5. Aprovação e Supervisão (CGE)

→ Aprovação institucional do plano e acompanhamento dos resultados.

---

3. Ciclo de Prestação de Contas

O ciclo de prestação de contas da gestão de riscos de TIC seguirá o seguinte calendário:

Período	Responsável	Atividade	Instância de Destino
Anual	STI	Relatórios de acompanhamento dos riscos estratégicos e táticos.	CGTIC
Anual	STI / CGTIC	Relatório consolidado de gestão de riscos de TIC.	CGE