

PLANO DE GESTÃO DE RISCOS DE TIC

2023-2026



AGÊNCIA NACIONAL DE ÁGUAS
E SANEAMENTO BÁSICO

AGÊNCIA NACIONAL DE ÁGUAS E SANEAMENTO BÁSICO
Ministério da Integração e do Desenvolvimento Regional

**PLANO DE GESTÃO
DE RISCOS DE TIC
2023 – 2026**

Brasília-DF
2024
2ª versão

Luís Inácio Lula da Silva
Presidente da República

Ministério da Integração e do Desenvolvimento Regional
Waldez Góes da Silva

Agência Nacional de Águas e Saneamento Básico

Veronica Sánchez da Cruz Rios
Diretora Presidente

Ana Carolina Argolo Nascimento de Castro
Diretora

Filipe de Mello Sampaio Cunha
Diretor

Marcelo Jorge Medeiros
Diretor Interino

Nazareno Marques Araújo
Diretor Interino

Superintendência de Tecnologia da Informação

Rafael Cunha Alves Moreira
Superintendente de Tecnologia da Informação

Mayara Nascimento de Farias Dutra de Andrade
Superintendente Adjunta

Marco Antônio Silva
Gerente executivo

Edher Garrido Lombardi
Coordenador da Superintendência de Tecnologia da Informação

Raphael Luiz Fonseca
Coordenador de Sistemas e Soluções

Francilene Faria Araújo Mendes
Coordenadora de Governança de Tecnologia da Informação

Edesio Ferreira da Silva Júnior
Coordenador de Operações e Infraestrutura de Tecnologia da Informação

Fabiano Costa de Almeida
Coordenador de Segurança da Informação e Comunicação

Alana Teles Nunes
Coordenadora de Planejamento e Projetos

Edison Moreira de Carvalho Junior
Coordenador de Gestão de Dados

Agência Nacional de Águas e Saneamento Básico – ANA
Setor Policial Sul, Área 5, Quadra 3, Blocos B, L, M, N, O e T
CEP: 70610-200, Brasília –DF
PABX: (61) 2109-5400 | (61) 2109-5252
Endereço eletrônico: www.ana.gov.br

Equipe de Apoio

Rafael Cunha Alves Moreira
Superintendente de Tecnologia da Informação

Mayara Nascimento de Farias Dutra de Andrade
Superintendente Adjunta de Tecnologia da Informação

Francilene Faria Araújo Mendes
Coordenadora de Governança de Tecnologia da Informação

José Carlos Tavares dos Anjos Filho
Coordenador substituto de Governança de Tecnologia da Informação

Ana Paula Moraes do Vale
Consultora de Governança

Igor Costa Souza de Almeida
Consultor de Gerenciamento de Projetos

Júlia Antunes Soares de Souza
Consultora de Gerenciamento de Projetos

Nádia Gleice da Silva
Consultora de Governança

LISTA DE FIGURAS

Figura 1 – Mapa Estratégico.....	9
----------------------------------	---

TABELAS

Tabela 1 - Nível de Risco (P x I.).....	12
Tabela 2 - Mapa de Calor Riscos de TIC.....	14

QUADROS

Quadro 1 - Documentos de Referência	8
Quadro 2 - Escala de Probabilidade	11
Quadro 3 - Escala de Impacto	11
Quadro 4 - Categorização Níveis de Risco	12
Quadro 5 – Siglas e termos.....	23

SUMÁRIO

LISTA DE FIGURAS.....	5
TABELAS.....	5
QUADROS.....	5
SUMÁRIO.....	6
1. APRESENTAÇÃO	7
2. DOCUMENTOS DE REFERÊNCIA.....	8
3. MAPA ESTRATÉGICO DE TIC	9
4. METODOLOGIA DE GERENCIAMENTO DE RISCOS DA ANA	10
5. RISCOS ESTRATÉGICOS DE TIC.....	13
6. MONITORAMENTO	22
7. RESPONSABILIDADES	23
8. SIGLAS E TERMOS	24

1. APRESENTAÇÃO

O gerenciamento de riscos auxilia as organizações a estabelecer estratégias, alcançar objetivos e tomar decisões fundamentadas, seguindo as diretrizes da norma ABNT NBR ISO 31000/2018. De acordo com essa norma, os riscos são definidos como os efeitos da incerteza que podem impactar positiva ou negativamente os objetivos organizacionais.

Na Agência Nacional de Águas e Saneamento Básico (ANA), conforme estabelecido pelas portarias N° 49 e 403 de 2019, foram implementadas a Política de Gestão de Riscos e a Metodologia de Gestão de Riscos. Esses documentos estabelecem princípios e diretrizes para a identificação, avaliação, tratamento e resposta aos riscos.

Durante a elaboração e revisão do Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) da ANA, foram analisados, identificados e avaliados os riscos que podem afetar o alcance dos objetivos de TIC na organização. O objetivo é monitorar e mitigar esses riscos ao longo do período de vigência do PETIC, estabelecido para 2023–2026.

2. DOCUMENTOS DE REFERÊNCIA

A lista de Documentos de Referência (Quadro 1) dispõe a relação dos normativos que estabelecem princípios e diretrizes a serem seguidos no mapeamento dos riscos de TIC da ANA.

Referência	Descrição
Portaria ANA nº 49/2019, de 8 de março de 2019	Aprova a Política de Gestão de Riscos da Agência Nacional de Águas e Saneamento Básico (ANA).
Portaria ANA nº 403/2019, de 27 de novembro de 2019	Aprova a Metodologia de Gestão de Riscos na Agência Nacional de Águas e Saneamento Básico (ANA).
PEI 2023–2026	Planejamento Estratégico Institucional (PEI)2023-2026.
PETIC 2023–2026	Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) 2023–2026.
ABNT NBR ISO 31000	Gestão de Riscos –Diretrizes.
MGR – SISF	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicação do Sistema do Sistema de Administração dos Recursos de Tecnologia da Informação do poder Executivo Federal.
Referencial básico de Gestão de Riscos.	Referencial básico de Gestão de Riscos – TCU.
Decreto nº 9.203, de 22 de novembro de 2017	Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.
MP/CGU N 01/2016	Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal

Quadro 1 - Documentos de Referência

3. MAPA ESTRATÉGICO DE TIC

O MAPA Estratégico de TIC, é uma ferramenta essencial para a STI buscar alinhamento entre a estratégia de negócio e o uso eficaz da tecnologia. Este mapa representa uma visão holística das metas e objetivos da ANA no que diz respeito à implementação e utilização de tecnologias de informação e comunicação. Ele identifica áreas-chave onde a TIC pode agregar valor, como melhorias na eficiência operacional, inovação de produtos e serviços, e aprimoramento da experiência do usuário final. Além disso, o Mapa Estratégico de TIC ajuda a estabelecer prioridades e alocar recursos de forma adequada, garantindo que os investimentos em tecnologia estejam alinhados com os objetivos estratégicos da Agência.

O Mapa Estratégico de TIC (Figura 1) é a tradução dos Objetivos e Referenciais Estratégicos definidos durante a elaboração e revisão do PETIC – com vigência de 2023 a 2026.

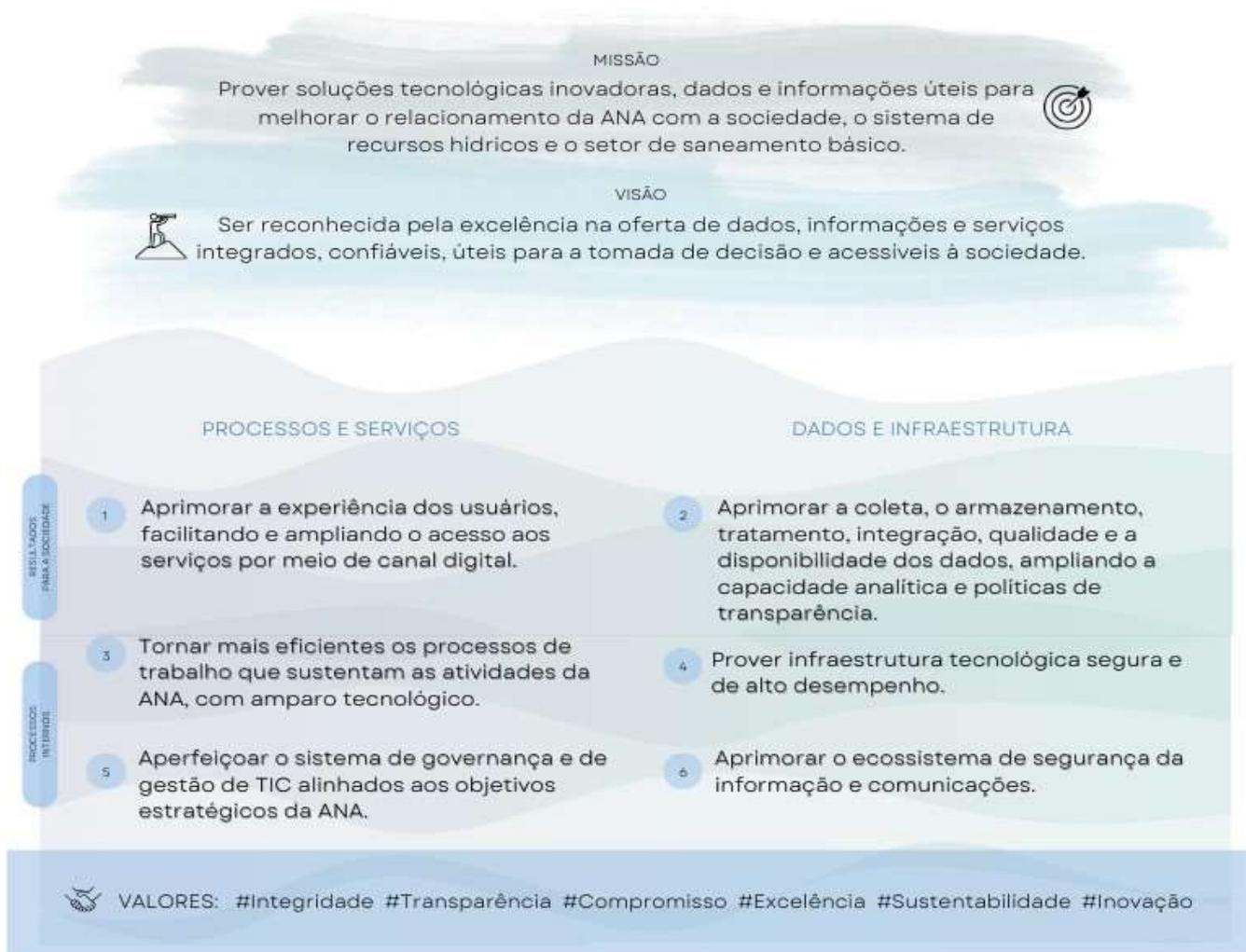


Figura 1 - Mapa Estratégico

4. METODOLOGIA DE GERENCIAMENTO DE RISCOS DA ANA

No âmbito da Agência Nacional de Águas (ANA), o gerenciamento de riscos foi instituído por meio da portaria N° 49, de 08 de março de 2019 – que aprova a Política de Gestão de Riscos.

Para a execução dos trabalhos, considerou-se também a Portaria n° 403, de 27 de novembro de 2019 – que aprova a metodologia de gestão de riscos. Esse documento define que o gerenciamento relacionado aos riscos deve ocorrer seguindo estas fases: Classificação e avaliação; Plano de Gestão de Riscos, além de Monitoramento do processo.

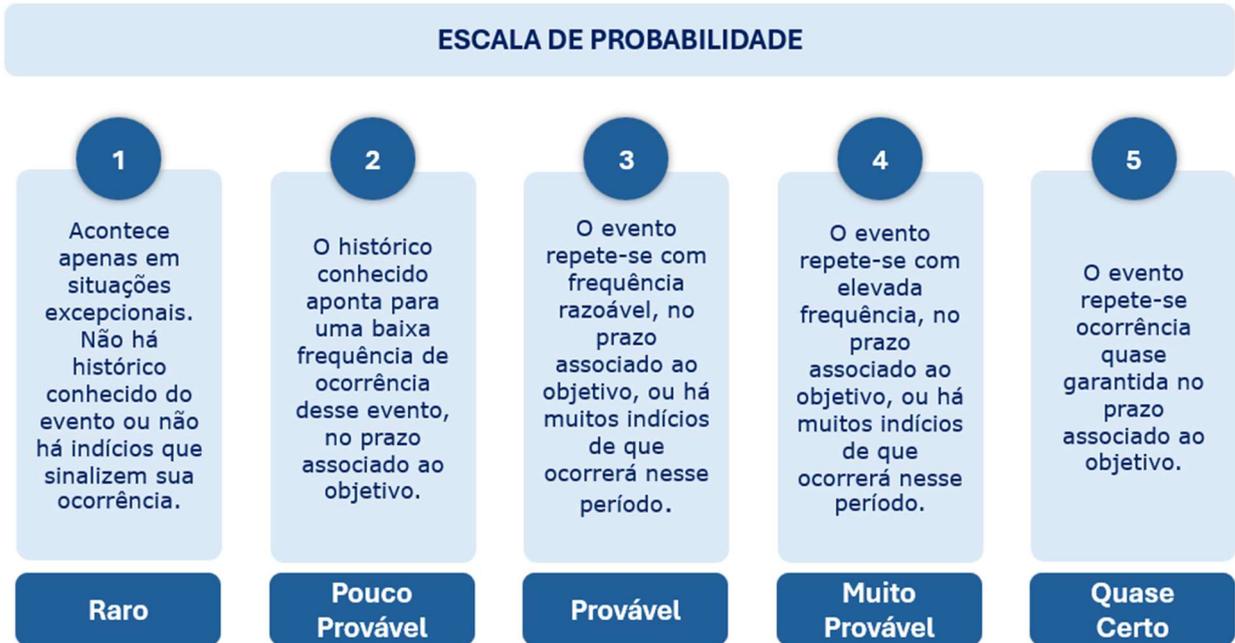
Conforme o Art. 5º da Metodologia de Gestão de Riscos da ANA, a etapa de “classificação e avaliação” compreende a identificação, análise e priorização tanto das iniciativas estratégicas quanto dos processos, em cada Unidade Organizacional (UORG).

No âmbito da STI, a aplicação da metodologia abrangeu as coordenações de TIC:

- Coordenação de Governança de TIC (COGTI);
- Coordenação de Planejamento e Projetos (COPRO);
- Coordenação de Sistemas e Soluções (COSIS);
- Coordenação de Gestão de Dados (COGED);
- Coordenação de Segurança da Informação (COSIC); e
- Coordenação de Infraestrutura e Operações de TIC (COOPI).

Ainda em relação à etapa de “classificação e avaliação”, para cada evento de risco, foram atribuídos valores de probabilidade e de impacto em caso da ocorrência do risco.

Nesse sentido, a probabilidade é entendida como a avaliação dos cenários, em adição às expectativas favoráveis ou não de ocorrência dos eventos de risco. Tal diagnóstico deve ser mensurado observando-se a seguinte escala (Quadro 2):



Quadro 2 - Escala de Probabilidade

O impacto, por sua vez, avalia o grau de importância do impacto possível caso ocorra o evento de risco identificado, e deverá ser avaliado através da seguinte escala (Quadro 3):



Quadro 3 - Escala de Impacto

Uma vez avaliados os critérios de probabilidade e impacto, a metodologia prevê a categorização do nível de risco (Tabela 1) nesta escala de valores:

IMPACTO	Muito alto	16	16	32	48	64	80
	Alto	8	8	16	24	32	40
Moderado	4	4	8	12	16	20	
Baixo	2	2	4	6	8	10	
Muito baixo	1	1	2	3	4	5	
			1	2	3	4	5
DESCRIÇÃO			Raro	Pouco provável	Provável	Muito provável	Quase certo
		PROBABILIDADE					

Tabela 1 - Nível de Risco (P x I)

A categorização dos níveis de risco (Quadro 4) obedeceu à seguinte escala:

Probabilidade x Impacto (P x I)	Categorização	Resposta
1 a 3	Risco Baixo	Aceitar
4 a 8	Risco Moderado	Transferir / Compartilhar
10 a 32	Risco Elevado	Mitigar / Reduzir
40 a 80	Risco Extremo	Evitar

Quadro 4 - Categorização Níveis de Risco

5. RISCOS E TIC

O levantamento dos riscos de TIC que podem afetar a estratégia da Agência foi realizado em conjunto com o processo de revisão do PETIC - 2023-2026, para o qual cada coordenação foi diretamente relacionada a um dos seis objetivos estratégicos de TIC. Durante o processo de revisão, cada coordenação realizou a indicação/atualização dos riscos relacionados ao objetivo trabalhado em sua área de atuação.

Durante o processo de revisão do PETIC – 2023-2026, uma das etapas cruciais foi a análise e revisão dos riscos envolvidos. Essa revisão foi fundamental para garantir que o plano estivesse alinhado com os objetivos estratégicos da Agência e pudesse lidar de maneira eficaz com os desafios potenciais que poderiam surgir ao longo do período contemplado.

Os riscos são elementos inevitáveis em qualquer empreendimento, especialmente em projetos de grande escala, como é o caso do PETIC. Portanto, identificar, avaliar e mitigar esses riscos são atividades essenciais para garantir o sucesso e a eficiência das iniciativas propostas.

Durante as oficinas de revisão, foram adotadas diversas abordagens para analisar os riscos. Uma delas foi a identificação dos riscos potenciais, levando em consideração tanto os fatores internos quanto externos que poderiam impactar a implementação do PETIC. Isso incluiu aspectos como mudanças regulatórias, avanços tecnológicos, questões orçamentárias, entre outros.

Após a identificação dos riscos, foi realizada uma análise mais aprofundada para avaliar sua probabilidade de ocorrência e o impacto que poderiam ter no plano estratégico. Além disso, foram desenvolvidas estratégias de mitigação para reduzir a probabilidade de ocorrência dos riscos mais significativos e minimizar seus impactos caso se concretizassem.

É importante ressaltar que a revisão dos riscos não se limitou apenas à fase inicial do processo de elaboração do PETIC. Pelo contrário, foi um exercício

contínuo ao longo de todo o período de implementação do plano. Isso porque as condições e o ambiente empresarial podem mudar rapidamente, o que requer uma constante reavaliação e adaptação das estratégias de mitigação de riscos.

Nesse sentido, destacamos ainda que o levantamento e a análise dos riscos fomentaram a elaboração de um Mapa de Calor de Riscos de TIC (Tabela 2). Essa ferramenta de comunicação visual dos riscos relacionados pelas coordenações, possibilita a pronta identificação de quais são os riscos extremos à Agência.

No caso da ANA, os riscos extremos corresponderam a **30%** dos riscos identificados. Observa-se a atenção para esse grupo nos Objetivos Estratégicos **1,3, 4, 5 e 6**.

IMPACTO	Muito alto	16	16	3	32	5	48	2	64	2	80
	Alto	8	8	2	16	5	24	2	32	3	40
Moderado	4	1	4	2	8	2	12		16		20
Baixo	2	2	2	3	4		6		8	3	10
Muito baixo	1	1	1	1	2	1	3		4		5
DESCRIÇÃO			1		2		3		4		5
			Raro		Pouco provável		Provável		Muito provável		Quase certo
		PROBABILIDADE									

Tabela 2 – Mapa de Calor Risco de TIC

Abaixo, nesta seção, constam listados todos os eventos de riscos identificados — incluindo suas respectivas avaliações, categorizações e ações de respostas.

OE 01: Aprimorar a experiência dos usuários, facilitando e ampliando o acesso aos serviços por meio do canal digital.

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER1	Perda de pessoas para outros contratos.	Operacional	Contrato com valores baixos e incompatíveis com o mercado.	Alta rotatividade de pessoas; perda de conhecimento.	4	8	32	Risco Alto	Mitigar / Reduzir
ER2	Dificuldades de comunicação entre a COSIS e as áreas de negócio.	Operacional	Pessoas diferentes para cada ação, sistema, ferramentas.	Atraso na entrega de novas funcionalidades ou do projeto; desmotivação da equipe, falta de rastreabilidade das demandas, retrabalho	3	4	12	Risco Alto	Mitigar / Reduzir
ER3	Atraso de cronogramas devido a estimativas inadequadas ou imprecisas.	Operacional	Escopo mal definido ou em constante mudança; estimativa de tempo e recurso inadequados; subestimação da complexidade técnica do projeto, falta de maturidade .	Atraso na entrega das novas funcionalidades ou do projeto.	5	2	10	Risco Alto	Mitigar / Reduzir
ER4	Falta de atualização tecnológica, levando à obsolescência ou incompatibilidade com novas plataformas.	Operacional	Custo elevado das atualizações, foco em resultado frente a perenidade do negócio; falta de equipe capacitada para a transição tecnológica.	Sistemas inseguros; falta de confiabilidade no sistema; dificuldade nas entregas de novas funcionalidades; problema de manutenção.	5	2	10	Risco Alto	Mitigar / Reduzir
ER5	Processos de negócio não mapeados ou desatualizados, dificultando na implementação dos sistemas.	Operacional	Falta de entendimento dos processos da área de negócio; falta de priorização no mapeamento do processo pela área de negócio; ausência da gestão dos processos.	Atraso na entrega das funcionalidades ou do projeto; alterações nas regras de negócio do sistema, retrabalho.	2	2	4	Risco Médio	Transferir / Compartilhar

OE 02: Tratamento, integração, qualidade e disponibilidade dos dados, ampliando a capacidade analítica e políticas de transparência.

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER6	Falta de orçamento para projeto de Engenharia e Governança de Dados em nuvem.	Financeiro	Corte e/ou Redução do orçamento.	Diminuição da arquitetura proposta; Desligamento da estrutura montada na nuvem.	2	16	32	Risco Alto	Transferir / Compartilhar
ER7	Falta de equipe para o Projeto Novo Hidro (Modelagem de Dados).	Operacional	Falta de contratação por ausências de recursos.	Não contratação.	8	3	24	Risco Alto	Transferir / Compartilhar
ER8	Falta de comprometimento das áreas de negócio envolvidas no Projeto Novo Hidro (Modelagem de Dados).	Operacional	Falta de envolvimento da área de negócio.	Atraso no processo de modelagem de dados.	2	8	16	Risco Alto	Transferir / Compartilhar
ER9	Falta de contrato para capacitação em solução Power BI.	Operacional	Falta de contratação por ausências de recursos.	Comprometimento na capacitação de servidores da agência na solução powerbi, impedindo a implantação da proposta de self-service BI.	2	2	4	Risco Médio	Aceitar
ER10	Falta de comprometimento da alta administração com o programa de governança de dados.	Estratégico	Falta de patrocínio da alta administração.	Atraso ou não execução do programa de governança de dados.	1	4	4	Risco Médio	Mitigar / Reduzir
ER11	Falta de comprometimento dos gestores com o comitê de governança de dados.	Estratégico	Falta de patrocínio dos representantes/área de negócio do comitê.	Atraso na execução do plano de ação do comitê de governança de dados.	2	4	8	Risco Médio	Mitigar / Reduzir
ER12	Curva de aprendizado maior com as soluções de dados definidas.	Operacional	Falta de equipe especializada em ciência de dados.	Atraso na execução das demandas de ciência de dados.	2	2	4	Risco Médio	Mitigar / Reduzir

OE 3:Tornar mais eficientes os processos de trabalho, que sustentam as atividades da ANA, com amparo tecnológico.

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER13	Conflitos de equipe ou problemas de comunicação que afetam a colaboração eficaz	Operacional	Ausência de alinhamento da gestão com os pontos focais de cada projeto; falta de acompanhamento transparente e eficaz; falta de conversas 1x1 de feedback.	Desmotivação da equipe; informação imprecisa ou errada; conflito entre as pessoas da equipe ou das equipes; perda de pessoal.	1	2	2	Risco Baixo	Aceitar
ER14	Dificuldade na gestão e fiscalização dos contratos	Operacional	Falta de definição das responsabilidades; falta de entendimento do processo de fiscalização e gestão.	Entregas com baixa qualidade; não realização das entregas previstas; dependência de pessoas com o conhecimento para fiscalizar o contrato, falta de conformidade.	3	8	24	Risco Alto	Mitigar / Reduzir
ER15	Ausencia de aplicação dos indicador para mensurar objetivamente as entregas dos contratos de desenvolvimento de sistemas (G4F e Logan)	Operacional	Ausência de previsão no contrato de um indicador; não utilização do indicador previsto no contrato por falta de ferramenta.	Entregas de baixa qualidade e quantidade; faturamento de empenho acima da quantidade de produtos entregues.	3	8	24	Risco Alto	Mitigar / Reduzir
ER16	Não continuidade do contrato de nuvem	Estratégico	Empresa manifestou pela renovação do contrato somente até agosto/2024.	Indisponibilidae dos sistemas que estão atualmente implantado na nuvem da AWS.	5	16	80	Risco Extremo	Evitar
ER17	Não contratação do SERPRO para manter os sistemas da ANA	Estratégico	Não conseguir orçamento; não realizar a contratação.	Mobilização das equipes para subir os sistemas novamente na infraestrutura da ANA.	3	16	48	Risco Extremo	Evitar

Qde	Evento de Risco	Categoria do Risco	Causa	Consequência	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER18	Mudança de Diretoria.	Estratégico	Mudança de Governo; Fim do exercício do mandato; Outros.	Mudança das diretrizes estratégicas.	1	2	2	Risco Pequeno	Aceitar
ER19	Alteração de normativos.	Conformidade	Ausência do apoio da alta administração e demais instâncias de aprovação	Não aprovação do mérito das contratações.	1	2	2	Risco Pequeno	Aceitar
ER20	Orçamento; Concorrência com outras contratações.	Financeiro	Falta de contratação por ausências de recursos.	Não contratação	2	5	10	Risco Alto	Mitigar / Reduzir
ER21	Mudança Tecnológica.	Operacional	Mudança tecnológica; Mão de obra capacitada.	Atraso na execução dos projetos; Ajustes nos contratos existentes; Atendimento as áreas prejudicadas; Dificuldade em contratar mão de obra capacitada.	3	1	3	Risco Pequeno	Aceitar
ER22	Processos indefinidos.	Operacional	Falta de processos.	Conflito de interesse na execução dos processos; Dificuldade na fiscalização dos contratos; Dificuldade nos processos de melhoria da infraestrutura.	5	8	40	Risco Extremo	Evitar
ER23	Auditoria Interna e Externa	Conformidade	Dificuldade de mensuração do contrato.	Suspensão do contrato de suporte de infraestrutura.	5	8	40	Risco Extremo	Mitigar / Reduzir

OE 05: Aperfeiçoar o sistema de governança e de gestão de TIC alinhados aos objetivos estratégicos da ANA.

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER24	Ausência de eficiência e eficácia nos processos de TI.	Operacional	Falta de processos definidos na STI.	Impede a STI de cumprir sua missão e alcançar seus objetivos e iniciativas propostos. Ausência de efetividade das entregas da STI.	3	4	12	Risco Alto	Mitigar / Reduzir
ER25	Implementação normativos internos e/ou externos com obrigatoriedade de prazos e ferramentas.	Conformidade	Obrigatoriedade Legal.	ANA não conforme com as normas estabelecidas por ela mesma; TI atrasar entregas planejadas devido ao cumprimento da norma.	2	16	32	Risco Alto	Aceitar
ER26	Não receber orçamento de acordo com o planejamento de TI.	Financeiro	Contingenciamento Orçamentário.	Os custos associados à infraestrutura de TIC, desenvolvimento de sistemas, manutenção e atualizações podem exceder os orçamentos previstos, levando a restrições financeiras e comprometendo a capacidade da ANA de atingir seus objetivos estratégicos.	3	16	48	Risco Extremo	Aceitar
ER27	Baixa execução do PETIC.	Planejamento	Falta de priorização das iniciativas estratégicas de TIC; Iniciativas não previstas no PETIC.	Impede a STI de cumprir as entregas previstas no PETIC.	3	8	24	Risco Alto	Mitigar / Reduzir
ER28	Falta de pessoal qualificado e Rotatividade.	Operacional	Processo Licitatório	A falta de pessoal qualificado, bem como a rotatividade de colaboradores-chave, representa um risco para a capacidade de entrega da STI.	3	8	24	Risco Alto	Mitigar / Reduzir
ER29	Não realizar a gestão de riscos de TIC.	Operacional	Não realizar a gestão dos riscos de TI.	Não tratar os riscos de TI pode resultar em consequências graves que afetam não apenas a segurança e a eficiência operacional da ANA, mas também sua reputação e sustentabilidade a curto a médio prazo. Portanto, é fundamental adotar uma abordagem proativa para identificar, avaliar e mitigar os riscos de TI, integrando a gestão de riscos à sua estratégia de negócios. Não aderente às práticas de Gestão de Risco.	3	16	48	Risco Extremo	Mitigar / Reduzir
ER30	Não conhecer as demandas de auditoria.	Conformidade	Falta de comunicação e alinhamento.	Não coletar as evidências solicitadas no prazo estabelecido; Não entregar as demandas de auditoria no prazo; Auditoria Incompleta ou Ineficaz; Sansões ou penalidades.	2	2	4	Risco Moderado	Mitigar / Reduzir

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER31	Falta de recursos orçamentários da STI.	Financeiro	Contigenciamento Orçamentário.	Necessidade de reprogramar as contratações de TIC.	2	16	32	Risco Alto	Aceitar
ER32	Falta de pessoal e equipe qualificada.	Operacional	Falta de alocação e falta de treinamento e capacitação.	Execução do processo de contratação e de gestão com baixa qualidade.	4	16	64	Risco Extremo	Mitigar / Reduzir
ER33	Execução inadequada do PCA.	Operacional	Não realizar planejamento adequado de contratação de TIC: falta de priorização na alocação de recursos e mudanças de prioridade de ações.	Não execução da estratégia de contratação de TIC da ANA.	3	16	48	Risco Extremo	Mitigar / Reduzir
ER34	Publicação de novos normativos de contratação de TIC.	Conformidade	Obrigatoriedade Legal.	Ocorrência de não conformidade normativa; Atraso nas entregas planejadas devido ao cumprimento da norma.	2	8	16	Risco Alto	Aceitar
ER35	Falha nos artefatos de contratação.	Operacional	Não aprimoramento dos processos de contratação e gestão de contratos.	Morosidade e/ou retrabalho no planejamento de contratação de TIC.	4	16	64	Risco Extremo	Mitigar / Reduzir

Qde	Evento de Risco	Categoria do Risco	Causa	Efeito	Probabilidade	Impacto	Nível de Risco		Resposta ao Risco
					Peso	Peso	PxI	Descrição	
ER36	Ausência do apoio da alta administração	Conformidade	Mudança de diretoria; Alteração de legislação; Repriorização do planejamento estratégico institucional;	Dificuldade para formalização dos artefatos gerados; Obtenção do engajamento das demais áreas de negócio; Compromete a avaliação da eficiência operacional.	2	4	8	Risco Moderado	Transferir / Compartilhar
ER37	Baixo envolvimento/engajamento dos servidores e colaboradores da ANA com as questões de segurança da informação	Operacional	Sobrecarga; Baixo engajamento; Desconhecimento da importância; Concorrência com outras atividades;	Baixa confiabilidade das informações que são documentadas no PCN ANA	4	8	32	Risco Alto	Evitar
ER38	Não implementação da ETIR Setorial (de Águas)	Conformidade	Ausência de engajamento/envolvimento das superintendências da ANA	Pode ocorrer ataques cibernéticos, invasões a instalações físicas das estações de tratamento de água; comando inadequado de portões de barragens; Ataques para cancelamento de cobranças e multas; Invasão de instalações para sabotagem. Vazamento de dados e aliciamento de pessoas para que atuem contra a instituição.	5	16	80	Risco Extremo	Evitar
ER39	Descontinuidade operacional dos processos de negócio	Operacional	Não publicação de Política e Plano de Continuidade de Negócio institucional	Interrupção no atendimento dos usuários finais.	3	16	48	Risco Extremo	Evitar
ER40	Falta de pessoas dedicadas para os processos de segurança da informação.	Operacional	Não priorização na alocação de recursos para área de Segurança da Informação e Comunicações	Falta de aquisição de tecnologias essenciais (execução do orçamento); Atrasos na reformulação de políticas de segurança; Exposição desnecessária a ameaças cibernéticas.	5	8	40	Risco Extremo	Evitar

6. MONITORAMENTO

O monitoramento de riscos de Tecnologia da Informação e Comunicação (TIC) na Agência Nacional de Águas (ANA) desempenha um papel fundamental na garantia da segurança, eficiência e continuidade das operações tecnológicas da instituição.

O monitoramento de riscos de TIC na ANA envolve a identificação, avaliação e tratamento dos riscos relacionados à:

- Processos de governança de TIC;
- Infraestrutura;
- Privacidade e Segurança da Informação;
- Sistemas,
- Dados;
- Contratações de TIC; e
- Processos tecnológicos utilizados pela Agência.

Essa prática permite antecipar possíveis vulnerabilidades, prevenir incidentes de segurança, assegurar a conformidade com normas e regulamentos específicos do setor e manter a integridade e disponibilidade das informações.

Além disso, o monitoramento de riscos de TIC na ANA contribui para a tomada de decisões estratégicas, permitindo que os gestores tenham uma visão abrangente dos potenciais impactos dos riscos tecnológicos sobre as atividades da agência. Dessa forma, é possível direcionar recursos de forma mais eficiente, priorizando ações de mitigação e investimentos em segurança da informação.

É importante ressaltar que esse monitoramento não deve onerar o processo, sendo realizado periodicamente, de acordo com a Metodologia de Gestão de Riscos de TIC, preferencialmente, de forma integrada com as Reuniões de Avaliação Estratégica da ANA – RAEs.

7. RESPONSABILIDADES

DIRETORIA



Responsável por aprovar o Plano de Gestão de Riscos de TIC e suas revisões. Além de assegurar a alocação dos recursos necessários à implantação do Plano de Gestão de Riscos de TIC.

CGDI



Validar, aprovar, propor e alterar documentos e processos da Governança de Riscos de TIC. A CGDI pode incluir, alterar e excluir riscos da carteira de riscos de TIC.

COGTI



Garantir a execução dos processos da Gestão de Riscos de TIC e realizar apoio técnico-metodológico.

COORDENAÇÕES



Executar os processos da Gestão de Riscos de TIC em relação aos riscos estratégicos e táticos, participar de Workshops, Oficinas, alimentar as ferramentas de Gestão de Riscos de TIC e implementar a gestão de riscos em sua unidade organizacional.

8. SIGLAS E TERMOS

Sigla	Descrição
ANA	Agência Nacional de Águas e Saneamento Básico
COGTI	Coordenação de Governança e Tecnologia da Informação
COPRO	Coordenação de Planejamento e Projetos
COOPI	Coordenação de Operação de Infraestrutura de Tecnologia da Informação
COGED	Coordenação de Gestão de Dados
COSIS	Coordenação de Sistemas Institucionais
PEI	Plano Estratégico Institucional
PETIC	Plano Estratégico de Tecnologia da Informação e Comunicação
STI	Superintendência de Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UORG	Unidade Organizacional
Probabilidade	A chance de que um evento ocorra, expressa em termos qualitativos ou quantitativos. Está relacionada à incerteza e à possibilidade de ocorrência de um evento indesejado que possa impactar os objetivos de uma organização.
Impacto	Como a consequência resultante da ocorrência de um evento indesejado, expressa em termos qualitativos ou quantitativos.
Evento de Risco	Efeito da incerteza, evento capaz de afetar positivamente (oportunidade) ou negativamente (ameaça) os objetivos, processos de trabalho, programas e projetos nos níveis estratégico, tático ou operacional.

Quadro 5 – Siglas e abreviações



AGÊNCIA NACIONAL DE ÁGUAS
E SANEAMENTO BÁSICO