

Instrução Normativa de Gestão de Riscos e Controles

Agosto de 2026

SUMÁRIO

1. OBJETIVO	4
2. ABRANGÊNCIA	4
3. DEFINIÇÕES	4
4. RESPONSABILIDADES	6
4.1 Conselho Deliberativo	6
4.2 Conselho Fiscal	6
4.3 Diretoria Executiva	7
4.4 Administrador Responsável pela Gestão de Riscos – ARGR	7
4.5 Unidade de Governança, Riscos e Compliance	7
4.6 Gestores e Donos dos Riscos	8
4.7 Empregados	9
4.8 Auditoria Interna	9
5. REGRAS GERAIS	10
5.1 Processo de Gestão de Riscos	10
5.2 Matriz de Riscos	10
5.3 Identificação dos Riscos e Oportunidades	11
5.3.1 Fontes de Risco	12
5.3.2 Categorias de Riscos	13
5.4 Análise dos Riscos	13
5.4.1 Avaliação do Impacto	13
5.4.2 Avaliação da Frequência/Probabilidade	14
5.4.3 Determinação do Risco Inerente ou Original	15
5.4.4 Identificação e Controles Elegíveis	15
5.4.5 Avaliação da Maturidade e Efetividade dos Controles	16
5.4.6 Cálculo da Efetividade Consolidada dos Controles	18
5.4.7 Determinação do Risco Resultante ou Residual	19
5.5 Avaliação do Risco	19
5.5.1 Respostas ao Risco	20
5.5.2 Tratamento e Governança Conforme o Nível do Risco	21

5.6	Monitoramento e Análise Crítica	22
5.7	Indicadores-Chave de Risco — KRIs	24
5.8	Incidentes de Risco	24
5.9	Registro, Evidências e Sistema de Gestão de Riscos	25
5.10	Comunicação e Reporte dos Riscos	26
6.	GESTÃO DE CONSEQUÊNCIA	27
7.	DOCUMENTOS DE REFERÊNCIA	27
8.	NOTAS EXPLICATIVAS	27
9.	APROVAÇÃO E VIGÊNCIA	27
10.	ANEXOS	28
11.	CONTROLE DE VERSÃO	28
	ANEXO I – CRITÉRIOS QUALITATIVOS DE IMPACTO	29
	ANEXO II – MATRIZ DE CONTROLES ELEGÍVEIS	32
	ANEXO III – CRITÉRIO DE AVALIAÇÃO DE RISCO E TRATAMENTO	33

1. OBJETIVO

Estabelecer diretrizes, responsabilidades, critérios e procedimentos para a identificação, análise, avaliação, tratamento, monitoramento, comunicação e reporte dos riscos e controles da Fundação, bem como para a identificação e o aproveitamento de oportunidades decorrentes das incertezas que possam contribuir para o alcance dos objetivos e para a geração ou preservação de valor.

2. ABRANGÊNCIA

Aplicável a todos os processos da Fundação Libertas.

3. DEFINIÇÕES

- a. **Apetite a Riscos:** Nível e tipo de risco que a Fundação está disposta a assumir ou manter para alcançar seus objetivos.
- b. **Causa:** Condição, circunstância, deficiência ou fator que pode favorecer ou contribuir para a ocorrência do evento de risco.
- c. **Consequência:** Resultado ou efeito decorrente da materialização do evento de risco.
- d. **Controle:** Ação, atividade, procedimento, mecanismo ou recurso implementado para prevenir, detectar, reduzir ou corrigir eventos de risco ou suas consequências.
- e. **Dono do Risco:** Gestor responsável pelo processo ou atividade ao qual o evento de risco está associado e que possui responsabilidade pela avaliação, resposta, tratamento e acompanhamento do risco, observadas as alçadas estabelecidas.
- f. **Efetividade do Controle:** Grau em que determinado controle se encontra adequadamente estabelecido e funciona, na prática, para prevenir, detectar ou reduzir o risco a que se destina.
- g. **Evento de Risco:** Situação ou acontecimento possível que, caso ocorra, possa afetar o alcance dos objetivos da Fundação.
- h. **Fonte de Risco:** Elemento que, isoladamente ou em combinação, possui potencial para originar ou influenciar a ocorrência de um risco.

- i. Frequência/Probabilidade: Expectativa de ocorrência ou repetição do evento de risco, considerando histórico, exposição, contexto atual e demais condições relevantes.
- j. Impacto: Magnitude das consequências decorrentes da materialização do evento de risco, avaliada conforme critérios qualitativos e, quando mensurável, quantitativos estabelecidos pela Fundação.
- k. Incidente de Risco: Materialização, total ou parcial, de evento de risco previamente identificado ou ocorrência que evidencie nova exposição relevante.
- l. KRI — *Key Risk Indicator*: Indicador-chave utilizado para acompanhar alterações na exposição ao risco ou identificar sinais de aumento, redução ou materialização do risco.
- m. Matriz de Riscos: Representação gráfica utilizada para determinar e visualizar o grau de exposição ao risco a partir da combinação entre os níveis de Impacto e Frequência/Probabilidade, segundo escalas de 1 a 5. O cruzamento dessas variáveis gera um score de 1 a 25, utilizado para classificar o risco nos graus Muito Baixo, Baixo, Médio, Alto ou Muito Alto, conforme os critérios estabelecidos neste normativo.
- n. Oportunidade: Circunstância, evento ou condição decorrente de incerteza que possa produzir efeito favorável sobre os objetivos da Fundação, contribuindo para geração ou preservação de valor, melhoria de processos, eficiência, inovação, sustentabilidade ou alcance de resultados.
- o. Peso do Controle: Valor atribuído ao controle de acordo com sua natureza e capacidade potencial de mitigação, conforme metodologia estabelecida nesta Instrução Normativa.
- p. Plano de Ação: Conjunto estruturado de medidas destinadas a implementar, fortalecer ou corrigir controles e reduzir a exposição ao risco.
- q. Risco Inerente ou Original: Nível de risco existente antes de considerar os efeitos dos controles associados ao evento.
- r. Risco Resultante ou Residual: Nível de risco remanescente após a consideração dos controles existentes e de sua efetividade.
- s. Risco: Efeito da incerteza sobre os objetivos, que pode resultar em ameaças ou oportunidades, representando desvios em relação aos resultados esperados pela Fundação.

- t. Tolerância ao Risco: Limite de variação aceitável em relação ao apetite estabelecido, dentro do qual a exposição pode ser admitida mediante condições específicas de governança e acompanhamento.
- u. Tratamento do Risco: Processo de seleção e implementação de medidas destinadas a modificar o risco.

4. RESPONSABILIDADES

4.1 Conselho Deliberativo

- a. Promover, no âmbito de suas competências, a importância da Gestão de Riscos e Controles em todos os níveis da Fundação.
- b. Aprovar a Política de Gestão de Riscos e demais diretrizes submetidas à sua competência.
- c. Aprovar o apetite e os limites de tolerância aos riscos, conforme critérios institucionais aplicáveis.
- d. Acompanhar os riscos relevantes e as exposições que demandem reporte ao Conselho, conforme as alçadas estabelecidas.
- e. Deliberar sobre a manutenção excepcional de exposições classificadas fora do apetite, observadas suas competências estatutárias.
- f. Acompanhar informações consolidadas sobre o ambiente de riscos, controles e medidas de tratamento relevantes.

4.2 Conselho Fiscal

- a. Acompanhar, no âmbito de suas atribuições, a adequação dos controles internos e dos mecanismos de gerenciamento de riscos.
- b. Considerar informações de riscos e controles no exercício de suas atividades de fiscalização.
- c. Recomendar, quando aplicável, medidas de aprimoramento dos controles e da gestão de riscos.

4.3 Diretoria Executiva

- a. Assegurar a implementação da Gestão de Riscos e Controles na Fundação.
- b. Promover ambiente organizacional favorável à identificação, comunicação e tratamento tempestivo dos riscos.
- c. Acompanhar os riscos classificados no limite de tolerância e acima do apetite.
- d. Deliberar sobre matérias de riscos submetidas à sua alçada.
- e. Avaliar a manutenção temporária de exposições acima do apetite, estabelecendo, quando aplicável, condições, responsáveis e prazos para reenquadramento.
- f. Assegurar recursos compatíveis com a natureza e criticidade dos riscos identificados.

4.4 Administrador Responsável pela Gestão de Riscos – ARGR

- a. Zelar pela implementação e pelo adequado funcionamento da estrutura de Gestão de Riscos da Fundação, observadas as políticas, metodologias, limites e demais diretrizes estabelecidas.
- b. Acompanhar o perfil de riscos da Fundação, com especial atenção às exposições classificadas no limite de tolerância, acima ou fora do apetite.
- c. Acompanhar a adequação dos mecanismos de identificação, análise, avaliação, tratamento, monitoramento e reporte dos riscos.
- d. Acompanhar a implementação das medidas de tratamento relacionadas aos riscos relevantes, especialmente aquelas destinadas ao reenquadramento de exposições acima ou fora do apetite.
- e. Apoiar a disseminação da cultura de riscos e controles, reforçando a responsabilidade dos gestores pela gestão dos riscos inerentes aos processos sob sua responsabilidade.
- f. Comunicar às instâncias competentes situações relevantes que possam comprometer a efetividade da Gestão de Riscos, a adequação dos controles ou o cumprimento dos níveis de exposição estabelecidos pela Fundação.

4.5 Unidade de Governança, Riscos e Compliance

- a. Coordenar e manter a metodologia corporativa de Gestão de Riscos e Controles.

- b. Orientar tecnicamente as áreas na identificação, análise, avaliação, tratamento e monitoramento dos riscos.
- c. Estabelecer critérios, escalas, parâmetros e instrumentos necessários à aplicação uniforme da metodologia.
- d. Adotar metodologias para identificar, avaliar, tratar e monitorar riscos, bem como orientar a identificação e avaliação de oportunidades relevantes, com o objetivo de contribuir para o alcance da estratégia da Fundação.
- e. Avaliar a consistência metodológica das informações registradas.
- f. Questionar e solicitar revisão de avaliações quando identificar ausência de fundamentação, inconsistência ou incompatibilidade com os critérios estabelecidos.
- g. Consolidar a visão corporativa dos riscos da Fundação.
- h. Monitorar riscos, controles, planos de ação, incidentes e indicadores relevantes.
- i. Reportar à Diretoria Executiva e ao Conselho Deliberativo as exposições conforme as alçadas estabelecidas.
- j. Propor aprimoramentos na metodologia e nos instrumentos de Gestão de Riscos e Controles.
- k. Promover ações de orientação, capacitação e disseminação da cultura de riscos.
- l. Manter evidências e registros necessários à rastreabilidade do processo de gestão integrada de riscos.

4.6 Gestores e Donos dos Riscos

- a. Gerenciar os riscos, controles e oportunidades relacionados aos objetivos das atividades e processos sob sua responsabilidade, promovendo sua identificação, análise, avaliação, tratamento ou aproveitamento, conforme aplicável.
- b. Validar eventos, fontes, causas e consequências.
- c. Realizar a avaliação de impacto e frequência/probabilidade.
- d. Identificar e manter atualizados os controles relacionados aos riscos.
- e. Avaliar a efetividade dos controles com base em evidências.
- f. Definir a resposta ao risco, observados o apetite, a tolerância e as alçadas estabelecidas.

- g. Elaborar e implementar planos de ação quando necessários.
- h. Designar responsáveis e estabelecer prazos adequados para as ações.
- i. Monitorar mudanças no contexto que possam alterar a exposição ao risco.
- j. Comunicar tempestivamente alterações relevantes, incidentes, falhas de controle e novas exposições.
- k. Manter evidências suficientes das avaliações, controles e ações realizadas.
- l. Identificar e comunicar oportunidades relevantes relacionadas aos processos sob sua responsabilidade e avaliar, quando aplicável, ações para seu aproveitamento.

4.7 Empregados

- a. Executar os controles sob sua responsabilidade conforme estabelecido.
- b. Comunicar ao gestor situações que possam representar risco, incidente, falha ou deficiência de controle.
- c. Colaborar com as avaliações e fornecer informações e evidências quando solicitadas.
- d. Participar das ações de capacitação e disseminação da cultura de riscos.

4.8 Auditoria Interna

- a. Avaliar, de forma independente e objetiva, a adequação e a efetividade dos processos de governança, Gestão de Riscos e controles internos da Fundação.
- b. Avaliar, por meio dos trabalhos de auditoria, a existência, o desenho, a implementação e o funcionamento dos controles internos relacionados aos processos examinados.
- c. Comunicar às instâncias competentes as deficiências, fragilidades ou oportunidades de melhoria identificadas nos processos de Gestão de Riscos e controles internos.
- d. Recomendar ações corretivas ou de aprimoramento decorrentes dos trabalhos realizados, preservada a responsabilidade da gestão pela definição e implementação das medidas.
- e. Acompanhar, conforme o Plano de Auditoria e os critérios aplicáveis, o tratamento das recomendações decorrentes dos trabalhos de auditoria.
- f. Considerar os riscos relevantes da Fundação como insumo para o planejamento dos trabalhos de auditoria, observada a abordagem baseada em riscos.

5. REGRAS GERAIS

5.1 Processo de Gestão de Riscos

A Gestão de Riscos da Fundação observará processo contínuo e integrado composto pelas seguintes etapas:



As avaliações devem ser fundamentadas em informações disponíveis, evidências, histórico, conhecimento técnico, contexto e julgamento profissional, evitando classificações baseadas exclusivamente em percepção subjetiva.

5.2 Matriz de Riscos

A Fundação adotará Matriz de Riscos 5×5 como instrumento para representação e classificação do nível de exposição dos eventos de risco. A Matriz de Riscos resulta do cruzamento entre o Impacto e a Frequência/Probabilidade, ambos avaliados em escala de 1 a 5, conforme os critérios estabelecidos nesta Instrução Normativa.

O score será obtido mediante a seguinte fórmula:

$$\text{Score do Risco} = \text{Impacto} \times \text{Frequência/Probabilidade.}$$

A representação gráfica deverá observar as faixas de classificação estabelecidas, de forma que cada célula da matriz corresponda ao score e ao respectivo grau de risco resultante da combinação entre Impacto e Frequência/Probabilidade.

IMPACTO	FREQUÊNCIA / PROBABILIDADE					GRAU DE RISCO	
	Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5		
Muito Alto 5,00	5 Baixo	10 Médio	15 Alto	20 Muito Alto	25 Muito Alto	 Muito Baixo Risco aceitável. Manter sob monitoramento de rotina.	1 a 4
Alto 4,00	4 Muito Baixo	8 Baixo	12 Médio	16 Alto	20 Muito Alto	 Baixo Risco aceitável. Monitorar periodicamente.	5 a 9
Médio 3,00	3 Muito Baixo	6 Baixo	9 Baixo	12 Médio	15 Alto	 Médio Risco no limite de tolerância. Requer atenção e ação gerencial.	10 a 14
Baixo 2,00	2 Muito Baixo	4 Muito Baixo	6 Baixo	8 Baixo	10 Médio	 Alto Risco acima do apetite. Exige plano de ação e acompanhamento.	15 a 19
Muito Baixo 1,00	1 Muito Baixo	2 Muito Baixo	3 Muito Baixo	4 Muito Baixo	5 Baixo	 Muito Alto Risco fora do apetite. Requer ação imediata e escalonamento.	20 a 25

A matriz será utilizada tanto para a determinação do risco inerente ou original, antes da consideração dos controles, quanto como referência para a classificação do risco resultante ou residual, após a aplicação da efetividade dos controles.

5.3 Identificação dos Riscos e Oportunidades

A identificação tem por objetivo reconhecer e descrever os eventos, circunstâncias e condições de incerteza que possam afetar os objetivos da Fundação, considerando tanto ameaças que possam

comprometer seu alcance quanto oportunidades que possam contribuir para melhores resultados, geração ou preservação de valor. A identificação deverá considerar, no mínimo:

- a. Processo.
- b. Evento de risco.
- c. Categoria de risco.
- d. Fonte de risco.
- e. Causas.
- f. Consequências.

Durante a identificação dos riscos, as áreas deverão avaliar, sempre que pertinente, se as circunstâncias analisadas também evidenciam oportunidades associadas ao processo, especialmente aquelas relacionadas à melhoria de eficiência, inovação, redução de custos, aprimoramento de controles, melhoria da experiência das partes interessadas, sustentabilidade, automação, aproveitamento de mudanças regulatórias ou outras condições favoráveis aos objetivos da Fundação.

5.3.1 Fontes de Risco

FONTE	REFERÊNCIA
Humano	Pessoas, competências, comportamento, erro, omissão ou conduta.
Processo	Fluxos, procedimentos, rotinas, desenho ou execução dos processos.
Tecnológico	Sistemas, infraestrutura, equipamentos, segurança ou recursos tecnológicos.
Terceiro	Fornecedores, prestadores, parceiros e demais terceiros.
Legislação/Regulador	Alterações, exigências ou obrigações legais e regulatórias.
Ambiente Externo	Condições econômicas, sociais, ambientais, políticas, setoriais ou outros fatores externos.

5.3.2 *Categorias de Riscos*

Os eventos serão classificados conforme sua natureza predominante, observadas as seguintes categorias:

- | | |
|--------------------------------|--|
| a. Risco Estratégico. | g. Risco Atuarial. |
| b. Risco Sistêmico. | h. Risco Legal e Integridade. |
| c. Risco Econômico-Financeiro. | i. Risco de Imagem e Reputacional. |
| d. Risco de Liquidez. | j. Riscos Ambientais, Sociais e de Governança — ASG. |
| e. Risco de Crédito. | k. Risco Operacional. |
| f. Risco de Mercado. | |

As definições completas das categorias e respectivos critérios qualitativos de impacto constam do **Anexo I**.

5.4 **Análise dos Riscos**

A análise tem por finalidade compreender a natureza e determinar o nível do risco, considerando:

- Impacto.
- Frequência/probabilidade.
- Risco inerente.
- Controles existentes.
- Efetividade dos controles.
- Risco resultante ou residual.

5.4.1 *Avaliação do Impacto*

O impacto deverá ser avaliado considerando a categoria do evento e a magnitude das consequências decorrentes de sua eventual materialização. A avaliação qualitativa observará os critérios específicos de cada categoria constantes do **Anexo I**.

Quando o evento puder gerar perda financeira direta mensurável, independentemente de sua categoria, poderá ser considerada também a métrica quantitativa:

NÍVEL DE IMPACTO.	PESO.	PERDA FINANCEIRA DIRETA.
 MUITO BAIXO.	1.	> Até R\$ 5.000,00.
 BAIXO.	2.	> Acima de R\$ 5.000,00 até R\$ 50.000,00.
 MÉDIO.	3.	> Acima de R\$ 50.000,00 até R\$ 150.000,00.
 ALTO.	4.	> Acima de R\$ 150.000,00 até R\$ 500.000,00.
 MUITO ALTO.	5.	> Acima de R\$ 500.000,00.

 Os valores de referência têm como base aproximadamente 0,01% do ativo da Fundação Libertas, considerando patrimônio de cerca de **R\$ 5 bilhões** (RAI 2025), equivalente a **R\$ 500.000,00.**

Um evento com perda financeira reduzida poderá apresentar impacto elevado ou muito alto em razão de consequência legal, atuarial, reputacional, estratégica ou de outra natureza.

Havendo mais de uma dimensão de impacto aplicável, deverá prevalecer, para classificação do evento, aquela que represente a consequência de maior severidade razoavelmente esperada, devidamente fundamentada, evitando subavaliação da exposição.

5.4.2 Avaliação da Frequência/Probabilidade

A frequência/probabilidade deverá representar a expectativa de ocorrência do evento nas condições existentes no momento da avaliação. Será considerado, como referência, o histórico de ocorrências dos últimos 12 meses, sem prejuízo da análise de outros fatores que possam aumentar ou reduzir a expectativa de ocorrência do evento.

PROBABILIDADE/ FREQUÊNCIA	PESO	EXPECTATIVA DA OCORRÊNCIA DO FATO (considerando o cenário atual, qual a expectativa do evento se materializar?)	FREQUÊNCIA DA ATIVIDADE (com qual frequência realizo a atividade que estou avaliando?)	HISTÓRICO DE EXPOSIÇÃO AO EVENTO DE RISCO (este evento já ocorreu nos últimos 12 meses, com abertura de incidente de risco ou não)
 Muito Baixa.	1	A ocorrência do evento é remota nas condições atuais.	 Até uma vez ao ano.	Não há histórico relevante. O evento seria esperado apenas em circunstâncias excepcionais.
 Baixa.	2	O evento pode ocorrer, mas sua ocorrência é pouco frequente.	 Anual a semestral.	Há alguma exposição ou histórico pontual, porém os elementos disponíveis indicam baixa possibilidade de ocorrência ou repetição.
 Média.	3	O evento é possível e existem condições concretas para sua ocorrência ou repetição.	 Trimestral, bimestral ou mensal.	Há histórico ou condições que tornam razoável considerar que o evento possa ocorrer ou se repetir periodicamente.
 Alta.	4	O evento tem elevada possibilidade de ocorrer ou se repetir.	 Quinzenal ou semanal.	Há histórico recorrente, condições atuais ou sinais consistentes que favorecem sua ocorrência ou repetição.
 Muito Alta.	5	O evento é esperado ou tende a ocorrer de forma muito frequente nas condições atuais.	 Mais de uma vez por semana, diária ou continuamente.	Há histórico significativo ou condições concretas que indicam elevada recorrência.

5.4.3 *Determinação do Risco Inerente ou Original*

O risco inerente representa a exposição existente antes da consideração dos controles. O *score* será determinado pela fórmula:

$$\text{Risco Inerente} = \text{Impacto} \times \text{Frequência/Probabilidade}$$

O resultado será posicionado na matriz 5×5 definida pela Fundação.

5.4.4 *Identificação e Controles Elegíveis*

Após a determinação do risco inerente, deverão ser identificados os controles existentes capazes de prevenir, detectar, reduzir ou corrigir o risco.

Não deverá ser considerado controle apenas porque determinada prática é desejável ou está prevista informalmente. Deve existir atividade ou mecanismo identificável e relacionado ao evento de risco.

Para fins de mensuração da capacidade de mitigação, os controles deverão ser enquadrados conforme sua natureza predominante, observados os critérios do **Anexo II** — Matriz de Controles Elegíveis.

O peso atribuído ao controle representa sua relevância potencial para mitigação do risco, não significando, isoladamente, que o controle seja efetivo.

A efetividade real deverá ser avaliada separadamente, considerando a forma como o controle se encontra implementado e funciona na prática.

Um mesmo controle não deverá ser cadastrado mais de uma vez para o mesmo evento apenas por produzir diferentes evidências ou possuir mais de uma característica.

Quando determinado controle apresentar características compatíveis com mais de uma tipologia, deverá ser adotado o enquadramento que melhor represente sua natureza predominante e forma efetiva de funcionamento, evitando duplicidade de benefício na redução do risco.

A mera existência de política, procedimento, contrato, sistema, relatório, treinamento ou outro instrumento não assegura, por si só, o reconhecimento integral do controle. Sua existência e funcionamento deverão ser verificáveis.

5.4.5 Avaliação da Maturidade e Efetividade dos Controles

Identificados os controles relacionados ao evento de risco, deverá ser avaliado o grau em que cada controle está estabelecido e funciona para prevenir, detectar ou reduzir o risco a que se propõe.

A avaliação deverá considerar a realidade do controle no momento da análise e ser sustentada, sempre que possível, por evidências verificáveis. Para avaliação serão utilizados os seguintes níveis:

 MÉTRICA DE EFETIVIDADE DOS CONTROLES			
NÍVEL DE EFETIVIDADE	PERGUNTA-CHAVE	CRITÉRIO OBJETIVO PARA ENQUADRAMENTO	REDUÇÃO DO RISCO INERENTE
 Inexistente	O controle existe?	O controle não existe ou há apenas uma prática informal, sem definição mínima de como, quando e por quem deve ser executada.	 0%
 Inicial	O controle é executado?	O controle existe e há alguma execução, porém ocorre de forma eventual, parcial ou dependente da iniciativa das pessoas, sem padrão suficiente para assegurar sua aplicação regular.	 25%
 Definido	O controle está estabelecido e é aplicado regularmente?	O controle possui forma de execução definida e é aplicado regularmente, com responsável e periodicidade identificáveis. Entretanto, ainda existem limitações relevantes de abrangência, evidência ou execução.	 50%
 Implementado	O controle funciona de forma consistente?	O controle está adequadamente implementado, é executado conforme definido e possui evidências suficientes de sua aplicação. Eventuais falhas são pontuais e não comprometem significativamente sua capacidade de mitigar o risco.	 75%
 Otimizado	Há evidências de que o controle efetivamente mitiga o risco?	Controle Efetivo. Além de funcionar de forma consistente, sua efetividade é acompanhada ou verificada por monitoramento, indicadores, testes, revisões ou outras evidências que demonstrem sua capacidade de prevenir, detectar ou reduzir o risco.	 85%

A classificação deverá refletir a efetividade observada, não apenas o desenho esperado do controle. A atribuição dos níveis Implementado ou Otimizado deverá possuir evidências suficientes que permitam demonstrar o funcionamento do controle.

A ausência de evidência suficiente deverá ser considerada na avaliação, ainda que a área informe que o controle é executado.

A avaliação de efetividade deverá ser revista quando houver:

- a. Alteração relevante no processo.
- b. Mudança no desenho ou execução do controle.
- c. Incidente de risco.
- d. Falha identificada no controle.
- e. Apontamento de auditoria ou fiscalização.
- f. Alteração normativa relevante.
- g. Mudança significativa na exposição ao risco.
- h. Evidência de que o controle não está produzindo o resultado esperado.

5.4.6 Cálculo da Efetividade Consolidada dos Controles

Quando houver mais de um controle associado ao mesmo evento, a efetividade consolidada será calculada mediante média ponderada, considerando:

- a. O peso elegível de cada controle.
- b. A efetividade atribuída a cada controle.
- c. A participação proporcional do controle no conjunto de controles elegíveis associados ao evento.

Para evitar que a quantidade de controles, por si só, produza redução artificial do risco, os pesos serão normalizados proporcionalmente pela soma dos pesos elegíveis dos controles considerados.

$$\text{Peso Aplicado Normalizado} = \text{Peso Elegível do Controle} \div \text{Soma dos Pesos Elegíveis dos Controles.}$$

A contribuição de cada controle será:

$$\text{Contribuição Ponderada} = \text{Efetividade Aplicada} \times \text{Peso Aplicado Normalizado.}$$

A efetividade consolidada será obtida pela soma das contribuições ponderadas dos controles:

$$\text{Efetividade Consolidada} = \Sigma (\text{Efetividade} \times \text{Peso Elegível}) \div \Sigma \text{Pesos Elegíveis.}$$

Somente controles ativos, relacionados ao evento e com avaliação de efetividade válida deverão produzir contribuição para o cálculo.

Controles sem avaliação de efetividade não deverão produzir redução automática da exposição.

5.4.7 Determinação do Risco Resultante ou Residual

O risco resultante ou residual representa a exposição remanescente após a consideração dos controles existentes e de sua efetividade.

O score será determinado pela seguinte fórmula:

$$\text{Score do Risco Resultante} = \text{Score do Risco Inerente} \times (1 - \text{Efetividade Consolidada dos Controles})$$

O risco resultante deverá ser classificado conforme as faixas estabelecidas pela Fundação e será utilizado como referência para a etapa de avaliação do risco.

A redução matemática do *score* não substitui a análise crítica do resultado. Quando houver indícios de que o resultado não representa adequadamente a exposição existente, o Dono do Risco deverá revisar os dados, controles, classificações e premissas utilizados.

5.5 Avaliação do Risco

A avaliação do risco é a etapa destinada a comparar o risco resultante com os critérios de apetite e tolerância estabelecidos pela Fundação, de modo a subsidiar a decisão quanto à necessidade e prioridade de tratamento.

Enquanto a análise do risco determina o nível de exposição, a avaliação do risco responde se essa exposição é aceitável para a Fundação e qual resposta deverá ser adotada.

A decisão deverá considerar, além do *score*:

- a. A natureza do risco.
- b. A materialidade das consequências.
- c. Obrigações legais e regulatórias.
- d. Interesses de participantes, assistidos, beneficiários, patrocinadores, instituidores e demais partes interessadas.
- e. Efetividade dos controles.
- f. Viabilidade e proporcionalidade de tratamentos adicionais.
- g. Interdependência com outros riscos.
- h. Mudanças relevantes no contexto interno ou externo.

Os critérios de avaliação e decisão aplicáveis ao risco resultante constam do **Anexo III**, contemplando o grau do risco, a posição frente ao apetite, a resposta ao risco, o tratamento e a governança, bem como a alçada de reporte e tolerância ao risco.

5.5.1 Respostas ao Risco

As respostas ao risco deverão ser selecionadas de acordo com a natureza e o nível da exposição.

- a. Aceitar: consiste em assumir conscientemente a exposição, mantendo os controles e o monitoramento aplicáveis, sem implementar tratamento adicional naquele momento. A aceitação não significa ausência de gestão ou monitoramento.
- b. Reduzir/Mitigar: Consiste em implementar, aperfeiçoar ou fortalecer controles e demais medidas destinadas a reduzir a probabilidade, o impacto ou ambos.
- c. Evitar: Consiste em eliminar a exposição mediante decisão de não iniciar, interromper ou modificar substancialmente a atividade que origina o risco.
- d. Compartilhar/Transferir: Consiste em compartilhar determinadas consequências ou responsabilidades com terceiros, por mecanismos como seguros, garantias, contratos ou outras estruturas adequadas. A transferência ou o compartilhamento não elimina a responsabilidade da Fundação pela adequada gestão do risco.

Quando a incerteza representar oportunidade para a Fundação, poderão ser adotadas, conforme aplicável, as seguintes respostas:

- a. Explorar: adotar medidas para viabilizar ou maximizar a realização da oportunidade.
- b. Potencializar: aumentar a possibilidade ou os benefícios decorrentes da oportunidade.
- c. Compartilhar: desenvolver a oportunidade em conjunto com terceiro que possua capacidade, recurso ou competência complementar.
- d. Aceitar: reconhecer a oportunidade sem adoção imediata de medida específica, mantendo-a sob acompanhamento quando pertinente.

5.5.2 Tratamento e Governança Conforme o Nível do Risco

Quando a avaliação indicar necessidade de tratamento, o Dono do Risco deverá definir medidas compatíveis com a natureza e magnitude da exposição.

O tratamento poderá compreender:

- a. Implantação de novos controles.
- b. Fortalecimento de controles existentes.
- c. Automatização de atividades.
- d. Revisão de processos.
- e. Alteração de responsabilidades ou alçadas.
- f. Segregação de funções.
- g. Capacitação.
- h. Revisão de normativos.
- i. Contratação ou revisão de garantias e seguros.
- j. Alteração de contratos.
- k. Implementação de indicadores ou mecanismos de monitoramento.
- l. Outras medidas consideradas adequadas.

O plano de tratamento deverá conter, no mínimo:

- a. Risco relacionado.

- b. Ação.
- c. Objetivo da ação.
- d. Responsável.
- e. Prazo.
- f. Situação.
- g. Evidência de conclusão.
- h. Resultado esperado, quando aplicável.

A conclusão formal da ação não implicará automaticamente redução do risco. A efetividade da medida deverá ser avaliada após sua implementação. Após a implementação do tratamento, o Dono do Risco deverá avaliar se a medida produziu o resultado esperado e, quando necessário, reavaliar os controles e o risco resultante. Caso o tratamento não produza redução compatível com o resultado esperado, deverão ser avaliadas medidas adicionais ou alternativas.

As oportunidades consideradas relevantes poderão resultar em ações, projetos, melhorias de processos, aprimoramento de controles ou outras iniciativas destinadas à sua exploração.

5.6 Monitoramento e Análise Crítica

O monitoramento constitui etapa contínua da Gestão de Riscos e tem por finalidade verificar se:

- a. O nível de exposição permanece adequado.
- b. Os controles permanecem existentes e efetivos.
- c. Os planos de tratamento estão sendo executados.
- b. As premissas utilizadas nas avaliações permanecem válidas.
- c. Ocorreram alterações relevantes no contexto.
- d. Surgiram novos riscos.
- e. Houve materialização de incidentes.

Constituem gatilhos para reavaliação, entre outros:

- a. Mudança relevante no processo.

- b. Alteração normativa ou regulatória.
- c. Mudança de sistema.
- d. Contratação ou substituição de terceiro relevante.
- b. Reestruturação organizacional.
- c. Falha de controle.
- d. Incidente de risco.
- e. Apontamento de auditoria, fiscalização ou órgão estatutário.
- f. Alteração significativa de indicadores.
- g. Redução da efetividade dos controles.
- h. Aumento da exposição.
- i. Mudança relevante no ambiente externo.

A periodicidade ordinária das reavaliações será anual, sem prejuízo de reavaliações extraordinárias sempre que identificado gatilho relevante capaz de alterar:

- a. As causas do risco.
- b. Suas consequências.
- c. O impacto.
- d. A frequência/probabilidade.
- e. Os controles existentes.
- f. A efetividade dos controles.
- g. O risco resultante.
- h. Sua posição frente ao apetite ou à tolerância.

O Dono do Risco não deverá aguardar o ciclo periódico de revisão quando tomar conhecimento de alteração relevante da exposição.

5.7 Indicadores-Chave de Risco — KRIs

Sempre que aplicável, os riscos relevantes deverão ser acompanhados por indicadores que permitam identificar alterações na exposição, sinais de materialização do risco ou redução da efetividade dos controles.

Os indicadores deverão ser definidos de forma objetiva e compatível com as informações disponíveis no processo, podendo considerar, entre outros:

- a. Ocorrência e recorrência de eventos ou incidentes.
- b. Erros, falhas, inconsistências ou retrabalhos.
- c. Descumprimentos de prazos ou obrigações.
- d. Falhas ou ausência de execução de controles.
- e. Reclamações ou manifestações relevantes.
- f. Perdas financeiras ou variações de valores relevantes.
- g. Indisponibilidade de sistemas ou serviços.
- h. Descumprimentos de terceiros.
- i. Atrasos em planos de ação.
- j. Outros indicadores capazes de demonstrar alteração relevante da exposição ao risco.

Quando o comportamento do indicador demonstrar aumento relevante da exposição, o Dono do Risco deverá avaliar a necessidade de revisar o risco, os controles ou as medidas de tratamento e, quando aplicável, comunicar à Unidade de Governança, Riscos e Compliance.

5.8 Incidentes de Risco

A materialização de risco deverá ser registrada quando relevante para permitir:

- a. Identificação do evento ocorrido.
- b. Data da ocorrência.
- c. Causas identificadas.
- d. Consequências.
- e. Impacto financeiro, quando mensurável.

- f. Controles que falharam ou foram insuficientes.
- g. Providências adotadas.
- h. Necessidade de reavaliação do risco.

A ocorrência de incidente poderá ensejar revisão da frequência/probabilidade, do impacto, dos controles, de sua efetividade e do tratamento definido.

5.9 Registro, Evidências e Sistema de Gestão de Riscos

As áreas deverão manter evidências suficientes para demonstrar:

- a. A fundamentação utilizada na identificação e avaliação dos riscos.
- b. Os critérios considerados para atribuição do impacto e da frequência/probabilidade.
- b. A existência e execução dos controles cadastrados.
- c. A fundamentação utilizada na avaliação da maturidade/efetividade dos controles.
- d. As decisões relativas à aceitação ou tratamento dos riscos.
- e. A implementação e conclusão dos planos de ação.
- f. O acompanhamento dos indicadores e demais mecanismos de monitoramento.
- g. As aprovações, justificativas e reportes exigidos pelas respectivas alçadas.

As informações registradas no Sistema de Gestão de Riscos deverão refletir a situação efetivamente existente no processo, não devendo ser mantidos controles, avaliações ou planos de ação que não correspondam à realidade operacional.

O Dono do Risco é responsável pela consistência das informações relativas aos riscos sob sua responsabilidade, sem prejuízo da atuação metodológica e do monitoramento realizados pela Unidade de Governança, Riscos e Compliance.

A Unidade de Governança, Riscos e Compliance poderá solicitar complementação, correção ou reavaliação de registros quando identificar:

- a. Inconsistência metodológica.

- b. Ausência ou insuficiência de fundamentação.
- b. Incompatibilidade entre a classificação atribuída e os critérios estabelecidos nesta IN.
- c. Ausência de evidências suficientes dos controles.
- d. Divergência entre o controle cadastrado e sua execução prática.
- e. Plano de ação incompatível com a criticidade da exposição.
- f. Outras situações que possam comprometer a qualidade ou a confiabilidade da Gestão de Riscos.

As alterações relevantes realizadas nas avaliações deverão preservar, sempre que tecnicamente possível, histórico e rastreabilidade suficientes para identificar a evolução do risco.

5.10 Comunicação e Reporte dos Riscos

A comunicação de riscos deverá permitir que as informações relevantes cheguem tempestivamente às instâncias com competência para conhecimento, acompanhamento ou decisão.

Os reportes deverão considerar, conforme aplicável:

- a. Principais riscos da Fundação.
- b. Evolução dos riscos resultantes.
- c. Riscos no limite de tolerância, acima ou fora do apetite.
- d. Efetividade dos controles.
- e. Planos de tratamento.
- f. Ações vencidas ou críticas.
- g. Incidentes relevantes.
- h. KRIs e respectivos limites.
- i. Mudanças significativas no ambiente interno ou externo.
- j. Tendências de aumento ou redução da exposição.

A Unidade de Governança, Riscos e Compliance deverá consolidar as informações de riscos para reporte às instâncias competentes, observadas as alçadas definidas neste normativo.

O reporte não transfere a responsabilidade do Dono do Risco pela gestão da exposição e implementação das medidas sob sua responsabilidade.

6. GESTÃO DE CONSEQUÊNCIA

Integrantes do quadro corporativo ou outros membros das Partes Interessadas que observarem quaisquer desvios às diretrizes deste normativo, poderão relatar o fato através do Canal de Ética, podendo ou não se identificar.

Internamente, o descumprimento das diretrizes deste normativo enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem conforme a respectiva gravidade do descumprimento.

7. DOCUMENTOS DE REFERÊNCIA

- a. Política de Gestão de Riscos.
- b. Instrução Normativa de Riscos de Investimentos.
- c. ABNT NBR ISO 31000:2018

8. NOTAS EXPLICATIVAS

A aplicação estruturada da metodologia para identificação, avaliação, aproveitamento e monitoramento das oportunidades será implementada gradualmente em ciclo específico, de forma a permitir o amadurecimento dos critérios, instrumentos e registros necessários à sua operacionalização.

9. APROVAÇÃO E VIGÊNCIA

Esta norma entra em vigor a partir da data de sua aprovação, revogadas todas as disposições em contrário.

Casos omissos ou exceções relacionadas a este Normativo devem ser comunicados à Unidade de Governança, Riscos e Compliance e deliberados pela Diretoria Executiva.

10. ANEXOS

ANEXO I – Critérios Qualitativos de Impacto

ANEXO II – Matriz de Controles Elegíveis

ANEXO III - Critério de Avaliação de Risco e Tratamento

11. CONTROLE DE VERSÃO

VERSÃO	AUTOR	APROVAÇÃO	DATA	ALTERAÇÃO
000	GECIR	DREX 718 ^a	02/06/2020	Criação do Documento
001	GECIR	DREX 807 ^a	24/01/2023	Atualização do documento
				Conteúdo Revisado sem alteração em 2024
002	GERCE	DREX 955 ^a	25/08/2026	Atualização do documento de acordo com a nova metodologia adotada pela Fundação.

ANEXO I – CRITÉRIOS QUALITATIVOS DE IMPACTO

NÍVEL DE IMPACTO	PESO	RISCO ESTRATÉGICO	RISCO SISTÊMICO	RISCO ECONÔMICO-FINANCEIRO
 MUITO ALTO Peso 5	5	Comprometimento significativo da sustentabilidade, continuidade, posicionamento institucional ou perenidade da Fundação, decorrente de decisão estratégica inadequada, execução insuficiente ou baixa capacidade de adaptação a crises externas e mudanças regulatórias, ambientais, econômicas, setoriais ou institucionais, com perda relevante de aderência ao direcionamento estratégico.	Crise sistêmica propagada, com efeitos em cadeia capazes de comprometer a estabilidade, a confiança ou o funcionamento do sistema e a continuidade institucional.	Desequilíbrio severo capaz de comprometer a sustentabilidade institucional, a capacidade de manter compromissos relevantes ou a eficiência estrutural de alocação de recursos.
 ALTO Peso 4	4	Decisão estratégica equivocada ou resposta insuficiente a mudanças de mercado, ambiente regulatório, crises externas, fatores ambientais, econômicos, setoriais ou necessidades das partes interessadas, com impacto relevante na sustentabilidade, posicionamento institucional, orçamento, metas ou diretrizes estratégicas, exigindo revisão por alçadas superiores.	Choque relevante no sistema fechado de previdência complementar ou ambiente regulatório/financeiro, com efeitos sobre confiança, operação, liquidez ou investimentos.	Desequilíbrio expressivo com impacto sobre orçamento, patrimônio, obrigações ou sustentabilidade financeira, exigindo deliberação superior e plano de correção.
 MÉDIO Peso 3	3	Decisão estratégica inadequada, resposta insuficiente ou baixa adaptação a fatores internos ou externos, com comprometimento parcial de objetivo, meta, iniciativa, posicionamento institucional ou capacidade de execução, exigindo replanejamento, reforço de recursos ou deliberação gerencial.	Evento externo com reflexo indireto sobre planos, patrocinadores, participantes, mercado ou regulação, exigindo análise técnica e medidas preventivas.	Desequilíbrio financeiro ou orçamentário relevante, exigindo reprogramação de despesas, receitas, custos, obrigações ou compromissos institucionais.
 BAIXO Peso 2	2	Atraso, ajuste limitado, decisão estratégica com impacto restrito ou fator externo de baixa exposição, afetando unidade, iniciativa, meta ou processo institucional, com possibilidade de correção no ciclo vigente e sem comprometimento relevante da estratégia ou da perenidade.	Instabilidade setorial restrita, com necessidade de acompanhamento preventivo, mas sem alteração relevante na operação, liquidez, investimentos ou confiança.	Perda, encargo ou desvio orçamentário limitado, com ajuste interno possível e sem comprometer o equilíbrio econômico-financeiro.
 MUITO BAIXO Peso 1	1	Desvio pontual, decisão estratégica de baixa relevância ou fator externo sem impacto perceptível nos objetivos institucionais, na sustentabilidade, no posicionamento ou na continuidade da Fundação. Correção interna sem necessidade de reprogramação relevante.	Sinal ou evento externo setorial monitorável, sem impacto perceptível na Fundação, nos planos ou nas partes interessadas.	Impacto financeiro imaterial ou absorvível na rotina, sem afetar orçamento, custos, patrimônio, compromissos ou eficiência na alocação de recursos.

NÍVEL DE IMPACTO	PESO	RISCO LIQUIDEZ	RISCO CRÉDITO	RISCO MERCADO	RISCO ATUARIAL
 MUITO ALTO Peso 5	5	Incapacidade de cumprir compromissos essenciais nas datas previstas, com impacto material em beneficiários, assistidos, fornecedores, planos ou credibilidade institucional.	Perda substancial ou irrecuperável de crédito, com baixa relevante, impacto material nos planos/carteira ou comprometimento da confiança na gestão dos recursos.	Perda severa na carteira em cenário extremo, com comprometimento material do resultado dos planos, solvência econômica ou cumprimento da política de investimentos.	Desequilíbrio atuarial severo capaz de comprometer a solvência, sustentabilidade do plano ou cumprimento das obrigações previdenciárias/assistenciais.
 ALTO Peso 4	4	Insuficiência relevante de recursos líquidos para compromissos previstos, exigindo medidas extraordinárias de liquidez, priorização de pagamentos ou desinvestimento desfavorável.	Descumprimento significativo de obrigação pecuniária, com perda provável relevante, deterioração de ativo ou necessidade de medida jurídica/contábil.	Perda relevante na carteira ou descasamento importante em relação à meta/benchmark, exigindo deliberação, plano de ajuste ou revisão de alocação.	Desequilíbrio atuarial relevante ou baixa aderência de premissas/metodologias, exigindo revisão técnica, plano de equacionamento, ajuste de contribuições ou reporte regulatório.
 MÉDIO Peso 3	3	Dificuldade moderada de caixa ou necessidade de liquidação/rebalanceamento não planejado, com risco de atraso pontual ou custo financeiro controlável.	Inadimplência ou rebaixamento relevante de contraparte, com constituição ou aumento de provisão e impacto parcial no resultado do plano/carteira.	Perda moderada em função de taxas, preços, índices ou câmbio, com necessidade de análise de VaR, stress, drawdown ou reenquadramento tático.	Inadequação moderada de premissas, hipóteses, metodologia ou base cadastral, com impacto mensurável em provisões, reservas, contribuições ou resultado atuarial.
 BAIXO Peso 2	2	Pressão temporária de caixa, sanável com remanejamento ordinário de recursos, sem atraso de obrigação relevante.	Perda esperada ou atraso limitado, com recuperação provável e impacto financeiro baixo, exigindo acompanhamento e eventual ajuste de provisão.	Varição adversa limitada na carteira, com impacto baixo frente a benchmark, meta ou limites, demandando apenas monitoramento.	Divergência limitada em premissa, cadastro, regulamento ou metodologia, com ajuste técnico possível e impacto baixo nas reservas ou contribuições.
 MUITO BAIXO Peso 1	1	Necessidade pontual de ajuste de fluxo sem atraso, sem resgate desfavorável e sem impacto no cumprimento dos compromissos.	Atraso, inadimplência ou deterioração de contraparte sem perda esperada relevante, sem necessidade de provisão ou baixa.	Oscilação adversa dentro da volatilidade esperada e limites de acompanhamento, sem impacto relevante no resultado ou aderência à política.	Inconsistência técnica pontual sem alteração relevante em provisões, reservas, contribuições ou obrigações atuariais.

NÍVEL DE IMPACTO	PESO	RISCO LEGAL E INTEGRIDADE	RISCO DE IMAGEM E REPUTACIONAL	RISCOS AMBIENTAIS, SOCIAIS E DE GOVERNANÇA — ASG	RISCO OPERACIONAL
 MUITO ALTO Peso 5	5	Violação grave, fraude, dolo, desvio ético ou descumprimento regulatório severo, com sanções administrativas, cíveis ou penais e comprometimento institucional.	Dano reputacional severo e prolongado, com ampla exposição pública/regulatória, perda de credibilidade e comprometimento da relação com partes interessadas.	Evento ASG severo, com violação relevante de governança, responsabilidade socioambiental ou direitos e deveres de partes interessadas, capaz de comprometer sustentabilidade e perenidade.	Falha crítica ou interrupção severa que compromete operações essenciais, segurança da informação, continuidade, patrimônio ou confiança institucional.
 ALTO Peso 4	4	Violação relevante com potencial de autuação, multa, ação judicial, dano reputacional ou responsabilização de pessoas/instâncias.	Repercussão negativa relevante junto a participantes, patrocinadores, instituidores, associações, imprensa ou órgãos fiscalizadores, com perda de confiança.	Falha relevante na consideração de critérios ASG, com impacto na reputação, conformidade, governança, investimentos ou relacionamento com partes interessadas.	Falha relevante que compromete operação, serviço essencial, dado, prazo regulatório ou continuidade, com impacto financeiro, legal ou reputacional significativo.
 MÉDIO Peso 3	3	Descumprimento legal, regulatório, contratual ou ético com potencial de questionamento, retratação, contingência, apuração ou medida disciplinar.	Repercussão externa moderada, com questionamentos de partes interessadas, necessidade de resposta institucional e reversão no médio prazo.	Gestão insuficiente de fator ambiental, social ou de governança com impacto em decisão, contratação, investimento, transparência ou relacionamento institucional.	Falha com impacto moderado na execução do processo, atendimento, prazos, informação, qualidade ou continuidade, exigindo correção estruturada.
 BAIXO Peso 2	2	Inobservância normativa ou contratual limitada, com correção interna, apontamento de auditoria ou plano de ação, sem sanção relevante.	Repercussão externa limitada entre participantes, assistidos, beneficiários ou parceiros, com baixa exposição e reversão no curto prazo.	Baixa aderência a critério ASG em processo ou decisão específica, com correção simples e sem exposição externa relevante.	Falha operacional controlável, com retrabalho ou atraso limitado e sem impacto relevante em patrimônio, participantes, beneficiários ou obrigações externas.
 MUITO BAIXO Peso 1	1	Descumprimento formal ou falha interna de baixa relevância, sem descumprimento legal material, dano a terceiros ou necessidade de comunicação externa.	Repercussão interna limitada, restrita a colaboradores ou gestores, com reversão imediata por comunicação ou correção pontual.	Lacuna ASG pontual, sem impacto relevante em processos, decisões, investimentos ou relações institucionais.	Falha pontual com retrabalho mínimo, sem impacto relevante no resultado do processo, no atendimento, na segurança da informação ou na continuidade.

ANEXO II – MATRIZ DE CONTROLES ELEGÍVEIS



CONTROLES ELEGÍVEIS

	Tipo de controle	Peso	Classificação da relevância do controle	Descrição	Observação técnica
 Conferência documentada	Controles operacionais simples	3%	Fraco	Conferência pontual ou rotineira documentada, como uso de checklist e roteiros.	Controle detectivo mais confiável quando possui periodicidade, responsável e evidência de execução.
 Atividade padronizada e normatizada	Controles normativos/procedimentais	7,00%	Moderado	Atividade padronizada e normatizada, por meio de Estatuto, Política, Regulamento, Regimento, Diretrizes, Instrução Normativa, Procedimento Operacional, Manuais, Cartilhas ou Fluxos.	Só deve abater risco quando o normativo estiver vigente, divulgado, aplicado e revisado periodicamente.
 Documentação formal vigente	Controles documentais, contratuais e administrativos	7,00%	Moderado	Existência de documento formal devidamente preenchido, assinado, vigente e aprovado pelas alçadas competentes, como contratos, aditivos, cláusulas contratuais, apólices de seguro, declarações, termos de responsabilidade, acordos, procurações, autorizações ou documentos equivalentes.	A efetividade depende de validade jurídica, vigência ativa, assinatura regular, alçada adequada, aderência ao objeto, rastreabilidade, guarda documental e monitoramento dos prazos.
 Monitoramento manual contínuo	Controles de monitoramento	7,00%	Moderado	Monitoramento manual contínuo, por meio de planilhas, gráficos, BI ou painéis, sem alertas ou decisões automatizadas.	Depende de atualização, análise humana, rotina formal e registro do acompanhamento realizado.
 Atividade realizada por terceiro especializado ou avaliação de cenário por área técnica	Controles técnicos/especializados	7,00%	Moderado	Atividade realizada por terceiro especializado, como monitoramento de mercado, segmento e obrigação técnica específica. Avaliação de cenário por área ou terceiro especializado, com emissão de parecer, relatório, defesa, estudo técnico ou consultoria.	Quando realizado por terceiro especializado, a especialização reduz risco técnico, mas exige supervisão interna, contrato, SLA e validação das entregas. Já a avaliação de cenário, pode ser mais forte quando subsidia decisão crítica, regulatória, jurídica, atuarial, assistencial ou de investimento.
 Treinamento, aculturação e sensibilização	Controles de capacitação e sensibilização	7%	Moderado	Ações de treinamento, aculturação, reuniões periódicas, Diálogos Diário, estratégias de comunicação e sensibilização.	Contribui para reduzir riscos ao fortalecer a cultura organizacional e disseminar conhecimento. Sua efetividade depende de periodicidade, público-alvo definido, conteúdo atualizado e evidências de realização e participação.
 Dupla checagem por profissional distinto ou validação por alçada superior competente	Controles de revisão, segregação e aprovação	15%	Forte	Dupla checagem por profissional distinto, do mesmo nível hierárquico ou superior, sem autonomia de aprovação. Validação por alçada superior, realizada por gerência, comitê ou órgão estatutário.	Ganha robustez quando há parametrização de função e registro formal da revisão. Controle forte para decisões críticas, desde que exista evidência formal, como aprovação, dta, parecer ou registro sistêmico.
 Avaliação periódica por órgão independente ou área técnica	Controles independentes ou de segunda/terceira linha	15%	Forte	Avaliação periódica por órgão independente ou área técnica, como auditoria interna, reporte periódico, auditoria externa ou inspeção de 2º nível de controle.	Controle robusto quando há reporte formal periódico, recomendações, plano de ação e acompanhamento das pendências.
 Controle por parametrização ou Configuração Sistêmica	Controles sistêmicos, tecnológicos e de configuração	15%	Forte	Controle implementado por meio de regra, parâmetro, configuração técnica ou sistêmica, com objetivo de garantir, restringir, bloquear, segmentar, validar ou direcionar acessos, operações, fluxos, documentos (ex: backup) ou comunicações.	Controle forte quando há parametrização formalizada, responsável técnico definido, documentação, rastreabilidade, evidência de funcionamento e revisão periódica. Pode ser considerado muito forte quando houver bloqueios automáticos, alertas, trilha de auditoria, monitoramento contínuo e baixa dependência de intervenção humana.
 Monitoramento automático ou automatizado	Controles de monitoramento	17%	Muito Forte	Monitoramento automático ou automatizado, com alertas, inteligência artificial, análise de dados em tempo real, gestão de fluxo de trabalho, decisões lógicas ou sugestões de ação por sistema inteligente.	Controle forte quando há parametrização adequada, trilha de auditoria, registro de alertas e tratamento das exceções.

ANEXO III – CRITÉRIO DE AVALIAÇÃO DE RISCO E TRATAMENTO

SCORE RESIDUAL	GRAU DO RISCO	POSIÇÃO FRENTE AO APETITE	RESPOSTA AO RISCO	TRATAMENTO E GOVERNANÇA	ALÇADA DE REPORTE E TOLERÂNCIA AO RISCO
0 a 4	Muito baixo	Dentro do apetite	Aceitar.	Manter os controles existentes e o monitoramento de rotina.	Gestor/Dono do Risco. Pode aceitar a exposição e mantê-la sob monitoramento de rotina. A GERCE realiza o acompanhamento no âmbito da gestão integrada de riscos.
5 a 9	Baixo	Dentro do apetite	Aceitar ou Reduzir/Mitigar.	A exposição pode ser aceita ou reduzida mediante aperfeiçoamento dos controles, quando pertinente e proporcional.	Gestor/Dono do Risco. Pode aceitar a exposição. A GERCE realiza monitoramento periódico e consolida as informações relevantes para reporte à DREX.
10 a 14	Médio	Limite de tolerância	Reduzir/Mitigar, Compartilhar/Transferir ou Aceitar mediante justificativa.	Avaliar formalmente alternativas de tratamento. A manutenção da exposição deverá ser justificada e monitorada.	DREX. A manutenção do risco no limite de tolerância requer ciência e acompanhamento da DREX, mediante reporte da GERCE. A aceitação deverá ser formalmente justificada pelo Dono do Risco.
15 a 19	Alto	Acima do apetite	Reduzir/Mitigar, Compartilhar/Transferir ou Evitar.	Implementar tratamento prioritário para redução da exposição, com formalização obrigatória por meio de plano de ação. A permanência acima do apetite deverá ser temporária e excepcional.	DREX, com reporte ao CODE. A DREX delibera sobre a manutenção temporária da exposição e as medidas de tratamento. A GERCE reporta ao CODE enquanto o risco permanecer acima do apetite.
20 a 25	Muito alto	Fora do apetite	Evitar ou Reduzir/Mitigar imediatamente. Compartilhar/Transferir, quando aplicável.	Adotar medidas imediatas para eliminar ou reduzir a exposição, com formalização obrigatória por meio de plano de ação. A continuidade da exposição deverá possuir caráter excepcional.	CODE. Escalonamento imediato à DREX e reporte ao CODE. A manutenção excepcional da exposição deverá ser submetida ao CODE, observadas suas competências estatutárias, com monitoramento intensivo pela GERCE até o reenquadramento.