

UNIVERSIDADE FEDERAL DO CEARÁ
SECRETARIA DE GOVERNANÇA

Tutorial para preenchimento da planilha de gerenciamento de riscos



2025



UNIVERSIDADE FEDERAL DO CEARÁ

SECRETARIA DE GOVERNANÇA

Preenchimento da planilha de gerenciamento de riscos TUTORIAL

ETAPA 1. FIXAÇÃO DE OBJETIVOS

A gestão de riscos visa levantar e tratar eventos que possam comprometer o alcance dos objetivos definidos pela Instituição. Dessa forma, a Etapa 1 do processo de gerenciamento de riscos consiste em examinar minuciosamente o objeto de análise (objetivo estratégico ou processo organizacional) à luz de seus ambientes interno e externo, identificando e detalhando os seus objetivos específicos. [\(PGR, 2022, p. 36\)](#).

Processo: Preencher com o nome do processo que está sendo gerenciado os riscos.

Objetivo do Processo:

- Objetivo Geral: Deve ser preenchido com a descrição do objetivo geral do processo.
- Objetivo Específico: Devem ser utilizados os objetivos estratégicos constantes do [Mapa Estratégico](#) da UFC. Pode ser indicado mais de um objetivo.

Figura 1. Exemplos de objetivo geral e específicos.

UFC Planilha de Gerenciamento de Riscos de Integridade - SECGOV	
Unidade:	Pró-Reitoria de Gestão de Pessoas (PROGEP)
Setor:	Divisão de Aposentadorias e Pensões (DIAPE)
Responsável pelo gerenciamento:	Indicar o nome do Gestor Responsável pelo Gerenciamento de Riscos
Processos	
Processo (indicar)	Objetivos do Processo (Geral e específicos) (descrever)
Pensão Civil por Morte	Analisar as solicitações de Pensão Civil por Morte de acordo com os requisitos legais. Garantir a excelência na gestão de pessoas.

ETAPA 2. IDENTIFICAÇÃO DE EVENTOS

Nesta etapa, a equipe técnica designada deve construir uma lista abrangente de eventos de risco que possam comprometer o alcance dos objetivos gerais e específicos estabelecidos. (PGR, 2022, p. 37).

- **Evento de risco:** evento que pode evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos identificados na Etapa 1 (Fixação de Objetivos);
- **Tipo do risco:** indica se o evento de risco é uma oportunidade ou uma ameaça;
- **Categoria do Risco:** diz respeito à origem dos fatores que influenciam o evento de risco, de acordo com a Política de Gestão de Riscos da UFC (PGR, 2022 Quadro 7);

Quadro 7 - Categorias de Risco.

CATEGORIA	DESCRIÇÃO
Estratégico	Eventos que ameacem diretamente os objetivos estratégicos organizacionais, afetando o alcance da sua visão e a sustentabilidade da instituição no longo prazo
Financeiros/ Orçamentários	Eventos que podem comprometer a capacidade da UFC de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária
Operacionais	Eventos que podem comprometer as atividades da UFC, normalmente associados a falhas, deficiência ou inadequação de processos internos, de pessoas, de infraestrutura e de sistemas
Legal / de Conformidade	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFC
Imagem/ Reputação	Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade da UFC em cumprir sua missão institucional;
Integridade	Eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela UFC

Fonte: Elaboração própria, 2020 (dados extraídos da Política de Gestão de Riscos da UFC).

- **Causas do risco:** fatores que desencadeiam a ocorrência do evento de risco;
- **Consequências do risco:** possíveis efeitos da ocorrência do evento de risco.

Figura 2. Exemplo de identificação de riscos.

Identificação dos Riscos							
Processo	Fase	Evento de Risco (indicar)	Tipo de Risco	Categoria	Tipo de Risco de Integridade	Causas (descrever)	Consequências (descrever)
Pensão Civil por Morte	Inicial	Acesso aos Sistemas da UFC por parte do servidor aposentado	Ameaça	Operacionais		Falta de comunicação entre os sistemas em uso	Desrespeito à LGPD
Pensão Civil por Morte	Inicial	Suborno para concessão de aposentadorias e pensões	Ameaça	Integridade	Corrupção	Agilidade ou retardamento de atividades do processo	Enriquecimento ilícito do servidor

ETAPA 3. AVALIAÇÃO DE RISCOS

Nesta etapa, a equipe técnica designada para atuar na gestão de risco da unidade deve avaliar os riscos para cada um dos eventos identificados na etapa anterior. Essa avaliação deverá ser realizada considerando os critérios de probabilidade e de impacto. (PGR, 2022, p.39).

- **Probabilidade:** chance de ocorrência de um determinado evento de risco;
- **Escala de Probabilidade:** critérios que serão utilizados para o julgamento da probabilidade de ocorrência do evento (PGR, 2022 Quadro 8);

Quadro 8 – Escala de Probabilidade.

PROBABILIDADE	DESCRIÇÃO (sem considerar os controles internos existentes)	PESO
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8

Muito alta	Praticamente certo. De forma inequívoca, o evento ocorrerá. As circunstâncias indicam claramente essa possibilidade.	10
------------	--	----

Fonte: Metodologia de Gestão de Riscos – Escala de Probabilidade (CGU, 2018).

- **Impacto:** avaliação da magnitude da ocorrência do evento perante os objetivos estratégicos da organização;
- **Escala de Impacto:** critérios que serão utilizados para o julgamento do impacto de ocorrência do evento ([PGR, 2022 Quadro 9](#));

Quadro 9 – Escala de Impacto.

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação / comunicação / divulgação ou de conformidade)	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Fonte: Metodologia de Gestão de Riscos – Escala de Impacto (CGU, 2018).

- **Risco Inerente:** pontuação resultante da multiplicação da probabilidade pelo impacto a um evento de risco, excluindo-se qualquer mecanismo de controle;

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

- **Classificação de Risco:** faixas de classificação utilizadas para o julgamento do nível de risco de cada evento ([PGR, 2022 Quadro 10](#));

Quadro 10 – Classificação de Risco.

CLASSIFICAÇÃO	FAIXA
Risco Baixo – RB	0 – 9,99
Risco Médio – RM	10 – 39,99
Risco Alto – RA	40 – 79,99
Risco	80 – 100

Fonte: Metodologia de Gestão de Riscos – Classificação do Risco (CGU, 2018)

- **Matriz de Risco:** matriz de possíveis resultados da combinação das escalas de probabilidade e de impacto ([PGR, 2022, Quadro 11](#));

Quadro 11 – Matriz de Risco.

		IMPACTO				
		Muito baixo 1	Baixo 2	Médio 5	Alto 8	Muito Alto 10
P R O B A B I L I D A D E	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE

Fonte: Metodologia de Gestão de Riscos – Matriz de Riscos (CGU, 2018)

- **Controles Internos:** mecanismos que reduzem ou podem reduzir a probabilidade de sua ocorrência ou de seu impacto. Os controles preventivos atuam sobre possíveis causas do risco, com o objetivo de prevenir sua ocorrência (ex. requisitos; checklists; capacitação de servidores, etc.). Os controles de atenuação e recuperação são executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. (ex. plano de contingência; tomada de contas especiais; procedimento apuratório, etc.);
- **Fator de Avaliação dos Controles:** pontuação atribuída a partir do julgamento da efetividade dos controles existentes de acordo com os critérios estabelecidos ([PGR, 2022, Quadro 12](#));

Quadro 12 – Fatores de Avaliação dos Controles Internos Existentes.

NÍVEL	DESCRIÇÃO	FATOR DE AVALIAÇÃO DOS CONTROLES
Inexistente	Controles inexistentes, mal desenhados ou mal implantados, isto é, não funcionais.	1
Fraco	Controles têm abordagens <i>ad hoc</i> , tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

Fonte: Metodologia de Gestão de Riscos – Níveis de Avaliação dos Controles Internos Existentes (CGU, 2018).

- **Risco Residual:** pontuação resultante da multiplicação do risco inerente pelo fator de avaliação dos controles. Para cada evento identificado, a equipe técnica designada deve calcular o nível de risco, a partir dos critérios de probabilidade e de impacto;

$$\begin{aligned}
 & \textit{Risco Residual} \\
 & = \\
 & \textit{Risco Inerente X Fator de Avaliação dos Controles}
 \end{aligned}$$

Figura 3. Exemplo de avaliação de riscos

Avaliação dos Riscos						
Evento de Risco	Probabilidade	P	Impacto	I	Risco Inerente (PxI)	Classificação do Risco Inerente
Acesso aos Sistemas da UFC por parte do servidor aposentado	Média	5	Médio	5	25	Risco Médio

Figura 4. Exemplo de avaliação de controles e risco residual.

Avaliação dos Controles			Risco Residual	
Controles Preventivos	Controles de atenuação e recuperação	Avaliação dos Controles	Classificação do Risco Residual	Data da Última Avaliação
Envio de lista dos servidores aposentados no mês à CORE/PROGEP	Retirada do acesso indevido	Mediano	Risco Médio	18/07/2024

ETAPA 4. RESPOSTA AOS RISCOS

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento e o tipo de resposta aplicável a cada caso. (PGR, 2022, Quadro 13, p. 44).

O quadro 13, (PGR, 2022), mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 13 – Diretrizes de priorização dos riscos a serem tratados.

CLASSIFICAÇÃO	AÇÃO NECESSÁRIA	EXCEÇÃO
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser objeto de Avaliação Estratégica, comunicado ao Comitê de Governança e ao Reitor e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Governança.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Comitê de Governança.

Fonte: Adaptado de Metodologia de Gestão de Riscos – Atitude perante o risco para cada classificação (CGU, 2018).

Para cada risco priorizado deve ser selecionada uma opção de tratamento. Essa escolha depende do nível de risco e dos custos associados à implementação dos controles, conforme quadro 14 (PGR, 2022).

Quadro 14 – Opções de Tratamento de Risco.

OPÇÃO DE TRATAMENTO	DESCRIÇÃO
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.
Mitigar	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo/benefício adequado.
	Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas nas etapas de Identificação e Avaliação de Riscos .
Compartilhar	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se identificar outra unidade que tenha mais robustez para tratá-lo ou compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades (internas ou externas) dispostas a compartilhar o risco com a UFC. Caso essa opção incorra na interrupção do processo organizacional, a decisão deve ser aprovada pelo Comitê de Governança, ou Câmara associada.

Fonte: Adaptado de Metodologia de Gestão de Riscos – Opções de Tratamento do risco (CGU, 2018).

Figura 5. Exemplo de resposta aos Riscos.

Respostas ao Risco					
Processo	Fase	Evento de Risco	Classificação do Risco Residual	Opção de Tratamento	Justificativa da escolha da opção de tratamento
Pensão Civil por Morte	Intermediária	Perda de prazo para preenchimento do sistema E-Pessoal	Risco Alto	Mitigar	A responsabilidade é compartilhada com a Unidade

ETAPA 5. ATIVIDADES DE CONTROLES INTERNOS

Se a opção de tratamento do risco for MITIGAR, COMPARTILHAR ou EVITAR, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade (plano de tratamento) e/ou de impacto do risco (plano de contingência) a um nível dentro ou mais próximo possível das faixas de risco “baixo” ou “médio”). (PGR, 2022 p. 45).

O Plano de Tratamento é um planejamento de ações para a implementação das medidas preventivas. Ele deve conter:

- Responsável pela implementação das medidas de tratamento, devendo indicar um servidor ou o cargo cujo designado seja automaticamente associado ao Plano de Tratamento;
- **Ações preventivas:** medidas que visam diminuir a probabilidade de ocorrência do evento;
- **Monitoramento:** periodicidade e/ou mecanismos adotados para verificar a implementação das ações;
- **Data prevista para o início da implementação;**
- **Data prevista para o término da implementação.**

Figura 6. Exemplo de plano de tratamento.

Plano de Tratamento							
Evento de Risco	Opção de Tratamento	Responsável pelo Tratamento	Data prevista para início da implementação	Data prevista para o fim da implementação	Status	Ações preventivas	Monitoramento
Perda de prazo para preenchimento do sistema E-Pessoal	Mitigar	PROGEP (DIAPE)	janeiro/25	março/25	Não implementado	Estabelecer o controle de datas para padronização do prazo para preenchimento e envio do Ato de E-Pessoal	Trimestral

Ainda nesta etapa, está prevista a elaboração do Plano de Contingência, que se trata de uma definição prévia das ações que serão tomadas caso um risco venha a se concretizar. Ele deve conter:

- **Gatilho:** situação que determina o início das ações de contingência;
- **Responsável:** indicação do gestor que deve ser imediatamente comunicado em caso de ocorrência do risco para que possa demandar a execução das ações de contingência.
- **Ações de contingência:** ações imediatas que devem ser executadas em caso de ocorrência do

evento, com o objetivo de atenuar seu impacto (consequências).

Figura 7. Exemplo de plano de contingência.

Plano de Contingência		
Gatilho <i>(descrever)</i>	Ações de Contingência <i>(descrever)</i>	Responsável
- Constatação do não envio ou envio com informações divergentes do Ato; - Constatação de Auditoria	- Estabelecer um plano de trabalho para atendimento das demandas acumuladas em relação aos Atos de E-Pessoal;	PROGEP (DIAPE)

Como continuidade desta etapa, **em caso de ocorrência do evento de risco**, a unidade deve realizar seu registro. Ocorrência de Riscos é a notação do evento de riscos quando o gatilho é acionado, isto é, quando o risco identificado na etapa 2 se concretiza. Importante salientar que o gestor da unidade, bem como os responsáveis pelo gerenciamento de riscos, plano de tratamento e contingência, equipe técnica designada e unidades, no caso de riscos compartilhados devem informar à Secretaria de Governança quando houver a ocorrência do evento de risco. No registro da ocorrência deve conter:

- **Evento de Risco:** evento que pode evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos identificados na Etapa 1 (Fixação de Objetivos);
- **Data da Ocorrência:** Data em que ocorreu o evento;
- **Descrição da Ocorrência:** Descrição da ocorrência de forma detalhada e sua relação com o evento de risco;
- **Responsável pela Solução:** Responsável pela implementação das medidas de tratamento e contingência, que deve ser um servidor ou o cargo cujo designado seja automaticamente associado a solução da ocorrência de riscos;
- **Solução:** Descrição detalhada das soluções adotadas para resolução do evento de risco;
- **Resultados:** Descrever de forma sucinta os resultados alcançados com a solução do evento de risco.

Observação: Destacamos que todas as explicações e conceitos constam detalhadamente no [Plano de Gestão de Riscos \(PGR\)](#) desta Universidade, em caso de dúvidas consultar o referido plano.