

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

## Sumário

1. Objetivo .....	3
2. Campo de Aplicação .....	3
3. Definições e Siglas .....	3
<b>3.1. Definições</b> .....	3
<b>3.2. Siglas</b> .....	4
4. Documentos de Referência .....	4
5. Descrição .....	6
<b>5.1. Gestão de Riscos</b> .....	6
<b>5.1.1. Papéis e Responsabilidades</b> .....	6
<b>5.1.2. Detalhamento</b> .....	9
<b>5.1.2.1. Metodologia de Gestão de Riscos</b> .....	9
<b>5.2. Controles Internos da Gestão</b> .....	15
<b>5.2.1. Papéis e Responsabilidades</b> .....	15
<b>5.2.2. Detalhamento</b> .....	16
<b>5.2.3. Dos Objetivos dos Controles Internos da Gestão</b> .....	18
<b>5.2.4. Da Estrutura dos Controles Internos da Gestão</b> .....	19
6. Disposições Gerais .....	21
7. Anexos .....	21

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 1 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

<b>Histórico de Revisão</b>			
<b>Versão</b>	<b>Data</b>	<b>Responsável</b>	<b>Observação</b>
01	09/04/2018	GRIC	RD nº 01/450 <sup>a</sup> de 09/04/2018

### Informações Adicionais

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 2 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

## 1. Objetivo

Estabelecer as regras que norteiam as atividades de Gestão de Riscos e de Gestão de Controles Internos na Empresa de Pesquisa Energética (EPE).

## 2. Campo de Aplicação

Aplica-se a todas as áreas da EPE.

## 3. Definições e Siglas

### 3.1. Definições

**Accountability** - Obrigação dos agentes ou organizações que gerenciam recursos públicos de assumir responsabilidades por suas decisões e pela prestação de contas de sua atuação de forma voluntária, assumindo integralmente a consequência de seus atos e omissões.

**Ameaças** - Indício de acontecimento desfavorável que possa afetar algum processo ou objetivo.

**Ativos de Informação** - Os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.


**Conformidade** - Cumprimento das legislações, normas e procedimentos.

**Desastre** - Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.

**Gestor de riscos** - É o responsável por assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da organização, monitora o risco ao longo do tempo de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados de acordo com a política de gestão de riscos e garante que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização. Na EPE tais atribuições serão cumpridas pelo Assessor da área de Gestão de Riscos e de Gestão de Conformidade (GRC).

**Gestor proprietário do risco** - Pessoa responsável pelo monitoramento do risco e pela execução das respostas apropriadas. Na EPE tais atribuições serão cumpridas pelos Superintendentes e/ou equivalentes e coordenadores de projetos e atividades críticas da organização.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 3 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

**Resiliência** - Poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

**Risco** - Possibilidade de que um evento ocorra e afete positiva ou negativamente a implementação das estratégias ou a realização dos objetivos da organização, sendo medido em termos de impacto e de probabilidades.

**Usuário** - Qualquer empregado ocupante de cargo efetivo, cargo em comissão, cedido, prestador de serviço terceirizado, estagiário ou qualquer outro indivíduo que tenha acesso, de forma autorizada, aos recursos computacionais da EPE.

**Vulnerabilidade** - Falha ou fraqueza de um procedimento, design, tecnologia, controles internos e correlatos que possa facilitar a ocorrência de um desvio de finalidade.

### 3.2. Siglas

**GCN** - Gestão de Continuidade do Negócio

**GR** - Gestão de Riscos

**GRC** - Gestor da área de Gestão de Riscos e de Gestão de Conformidade

## 4. Documentos de Referência


- Lei 13.303, de 30 de junho de 2013: Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
- Código de Conduta da Alta Administração Federal, publicado no D.O.U. de 22 de agosto de 2000.
- Decreto nº 4.081, de 11 de janeiro de 2002: Institui o Código de Conduta Ética dos Agentes Públicos em exercício na Presidência e Vice-Presidência da República.
- IN 01/2016 MP-CGU: Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.
- CGPAR nº 18: Dispõe sobre diretrizes e recomendações para as Empresas Estatais relacionadas à políticas de Conformidade e Gerenciamento de Riscos.
- GSI IN1 NC4/2013: Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 4 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- GSI IN1 NC11/2012: Estabelecer diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta.
- ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
- ABNT NBR ISO 15999-1:2007: Fornece uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização além de obter confiança nos negócios da organização com clientes e outras organizações. Ela permite também que a organização avalie sua capacidade de GCN de uma maneira consistente e reconhecida.
- ABNT NBR ISO 31000:2009: Fornece princípios e diretrizes genéricas para a gestão de riscos.
- ABNT NBR ISO 31010:2012: Fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.
- ABNT NBR ISO 27005:2011: Fornece diretrizes para o processo de gestão de riscos de segurança da informação.
- COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.
- Política de Gestão dos Estudos e Pesquisas de Planejamento Energético: Estabelece orientações estratégicas sobre as práticas de Gestão dos Estudos e Pesquisas do Planejamento Energético, adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.
- Política de Pessoas: Estabelece orientações estratégicas sobre as práticas de Gestão de Pessoas adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.
- Política de Aquisições: Estabelece orientações estratégicas sobre as práticas de Gestão das Aquisições adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.
- Política de Informações: Estabelece orientações estratégicas sobre as práticas de Gestão da Informação adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.
- Política de Segurança da Informação e Comunicações: Estabelece orientações estratégicas sobre as práticas de Segurança da Informação e Comunicações adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 5 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- Política de Tecnologia da Informação e Comunicações: Estabelece orientações estratégicas sobre as práticas de Gestão da Tecnologia da Informação e Comunicações adotadas para o cumprimento da Missão e o alcance da Visão da Empresa.
- Metodologia de Gestão de Riscos EPE: Apresenta a abordagem sistemática do processo de Gestão de Riscos (GR) da EPE, visando manter os riscos em níveis aceitáveis e agregar valor ao negócio.
- Código de Ética e Conduta da EPE.

## 5. Descrição

### 5.1. Gestão de Riscos

Compreende a gestão de eventos ou condições de incerteza que, se ocorrerem, acarretarão em um efeito negativo sobre um ou mais objetivos planejados pela Empresa.

A Gestão de Riscos (GR) é o processo que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os objetivos e estratégias de negócio e os ativos de informação da Empresa, e equilibrá-los com os custos operacionais e financeiros envolvidos. É uma atribuição da Gestão de Riscos.

#### 5.1.1. Papéis e Responsabilidades


##### Conselho de Administração

- Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Empresa, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude.
- Garantir a existência de mecanismos que assegurem a essas áreas atuação independente.
- Deliberar sobre as questões estratégicas concernentes ao processo de gestão de riscos, tais como o grau de apetite a riscos da empresa, suas faixas de tolerância.
- Analisar os relatórios periódicos elaborados pela área de Governança, Riscos, Integridade e Controles Internos.

##### Diretoria Executiva

- Aprovar programa orçamentário específico para as ações de Riscos e Conformidade.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 6 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	


	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- Aprovar o Plano de Tratamento de Riscos.
- Promover as ações necessárias à manutenção da Gestão de Riscos e Conformidade.
- Promover a capacitação de recursos humanos para o desenvolvimento de competência tecnológica em Riscos e Conformidade.
- Analisar os relatórios periódicos elaborados pela Área de Governança, Riscos, Integridade e Controles Internos.

### **Área de Governança, Riscos, Integridade e Controles Internos (GRIC)**

- Propor políticas de Conformidade e Gerenciamento de Riscos para a empresa, as quais deverão ser periodicamente revisadas e aprovadas pelo Conselho de Administração, e comunicá-las a todo o corpo funcional da EPE.
- Propor, acompanhar, manter atualizadas e difundir as normas e metodologias de Gestão de Riscos e de Controles Internos da Gestão para a Empresa.
- Verificar a aderência da estrutura organizacional e dos processos, produtos e serviços da empresa às leis, normativos, políticas e diretrizes internas e demais regulamentos aplicáveis.
- Comunicar à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria a ocorrência de ato ou conduta em desacordo com as normas aplicáveis à empresa.
- Verificar a aplicação adequada do princípio da segregação de funções, de forma que seja evitada a ocorrência de conflitos de interesse e fraudes.
- Verificar o cumprimento do Código de Conduta e Integridade, conforme art. 18 do Decreto nº 8.945, de 27 de dezembro de 2016, bem como promover treinamentos periódicos aos empregados e dirigentes da empresa sobre o tema.
- Promover treinamentos periódicos para o desenvolvimento contínuo dos empregados e dirigentes da Empresa e incentivar a adoção de boas práticas de governança, gestão de riscos e controles internos.
- Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa.
- Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos.
- Estabelecer planos de contingência para os principais processos de trabalho da EPE.
- Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 7 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

 Empresa de Pesquisa Energética	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

- Disseminar a importância da Conformidade, da Integridade e do Gerenciamento de Riscos, bem como a responsabilidade de cada área da empresa nestes aspectos.
- Atuar direta ou indiretamente na avaliação de riscos ligados a corrupção e fraude e diretamente na posterior definição dos padrões e políticas de integridade da EPE.
- Atuar na orientação e treinamento dos colaboradores, por meio de consultorias técnicas, esclarecimento de dúvidas e realização de atividades de capacitação.
- Atuar diretamente ou de forma auxiliar na investigação de situações suspeitas de violação das normas de integridade.
- Auxiliar e orientar as diversas áreas da empresa na implementação das políticas e procedimentos de integridade.
- Recomendar à direção medidas necessárias para a correção de deficiências no programa ou para a remediação de irregularidades encontradas.
- Monitorar o programa de integridade, seja propondo metodologias de monitoramento, seja aplicando diretamente essas metodologias, e rever o programa periodicamente.
- Coordenar os instrumentos do Programa de Integridade, visando a sua efetividade.
- Promover a Guarda e gestão das experiências e capacidades acumuladas pela empresa em matéria de integridade.
- Monitorar a execução do modelo de Governança Corporativa, e de Gestão da EPE.
- Outras atividades correlatas definidas pelo Presidente.

#### **Gestor da área de Governança, Riscos, Integridade e Controles Internos (GRIC)**

- Coordenar a área de Governança, Riscos, Integridade e Controles Internos (GRIC).
- Indicar responsáveis pelo gerenciamento de atividades do Plano de Tratamento de Riscos.

#### **Superintendentes e/ou equivalentes e coordenadores de projetos e atividades críticas da organização**

- Gerenciar, orientar, mapear, avaliar e mitigar os riscos.
- Assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da Empresa.
- Elaborar relatórios a serem encaminhados para a área de GRIC, em cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 8 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	



	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

## Diretorias

- Designar o representante da diretoria para integrar o CR.
- Analisar os relatórios periódicos enviados pela área de GRIC.

## Usuários

- Observar e seguir as recomendações, normas e procedimentos de Conformidade e de Riscos. Solicitar orientações quando necessário.

## 5.1.2. Detalhamento

### 5.1.2.1. Metodologia de Gestão de Riscos

A partir desse momento fica instituída a Metodologia de Gestão de Riscos na EPE (documento Anexo).

As principais etapas do modelo de gerenciamento de riscos na EPE são:

- Identificação dos Riscos;
- Análise dos Riscos;
- Avaliação dos Riscos;
- Tratamento dos Riscos;
- Monitoramento e Análise crítica; e
- Comunicação e Consulta.


Segue detalhamento de cada uma das etapas:

#### Identificação dos Riscos

Na etapa de identificação deve-se observar que:

- A identificação é de responsabilidade primária dos gestores das áreas.
- Qualquer empregado que identifique um evento que potencialize um risco deverá comunicar imediatamente ao seu gestor imediato.
- Os riscos identificados devem ser devidamente registrados.
- Para a identificação dos riscos que possam afetar os objetivos da EPE devem ser considerados: a causa, a consequência e a sua tipologia.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 9 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

## Análise dos Riscos

Na etapa de análise deve-se observar que:

- A análise de riscos deve fornecer uma entrada para a avaliação de riscos e para as decisões sobre a necessidade dos riscos serem tratados e sobre as estratégias e métodos mais adequados de tratamento de riscos.
- A análise de riscos deve envolver a apreciação das causas e as fontes de risco, seus impactos positivos e a probabilidade de que esses riscos possam se materializar.

Detalha-se abaixo a tabela de níveis de probabilidade que devem ser observadas na EPE:

**Tabela 1 - Níveis de Probabilidade.**


Probabilidade	Descrição	Valor
Muito baixa	Muito improvável de ocorrer	1
Baixa	Improvável de ocorrer	2
Média	Ocorre ocasionalmente	3
Alta	Provável de ocorrer	4
Muito Alta	Ocorre frequentemente	5

Observa-se abaixo a tabela de níveis de impacto que devem ser observadas na EPE:

**Tabela 2 - Tabela de Níveis de Impacto.**

Impacto	Descrição	Valor
Desprezível	Os danos são insignificantes para a empresa	1
Baixo	A empresa consegue reparar os danos com seus próprios recursos	2
Crítico	A recuperação dos danos extrapola os recursos da empresa	3

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 10 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

Grave	Danos que venham a prejudicar a imagem da empresa ou gerem algum incidente grave	4
Gravíssimo	Destruição irreparável da imagem da empresa e/ou oferece risco de morte dos seus empregados	5


### Avaliação dos Riscos

Para a avaliação dos riscos devem ser considerados: o fator de probabilidade quanto à ocorrência e o fator de impacto que o risco possa causar, sendo estes graduados por meio da Matriz de Avaliação de Riscos.

**Tabela 3 - Matriz de Probabilidade e Impacto.**

		PROBABILIDADE				
		Muito Baixa (improvável) Nível 1	Baixa (Pouco provável) Nível 2	Média (Possível) Nível 3	Alta (Provável) Nível 4	Muito Alta (Frequente) Nível 5
<b>Impacto</b>	Desprezível Nível 1	1	2	3	4	5
	Baixo Nível 2	2	4	6	8	10
	Crítico Nível 3	3	6	9	12	15
	Grave Nível 4	4	8	12	16	20
	Gravíssimo Nível 5	5	10	15	20	25

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 11 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

 Empresa de Pesquisa Energética	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

Os controles requeridos e os níveis de conhecimento devem observar a criticidade do risco, conforme tabela abaixo:

CRITICIDADE	DESCRIÇÃO DO RISCO/CONTROLE REQUERIDO	CONHECIMENTO DO RISCO
<b>ALTA (15 A 25)</b>	Risco intolerável.  Ações imediatas devem ser implementadas e o monitoramento deve ser contínuo.	<ul style="list-style-type: none"> <li>• Diretor da área e ao Presidente</li> <li>• Diretoria Executiva e/ou CA</li> </ul> (para riscos com impacto direto no atingimento dos objetivos estratégicos)
<b>MÉDIA (5 A 12)</b>	Risco intolerável.  Ações devem ser implementadas e o monitoramento deve ser periódico.	<ul style="list-style-type: none"> <li>• Diretor</li> </ul>
<b>BAIXA (1 A 4)</b>	Risco tolerável.  Manter e aprimorar os controles existentes e monitorar para verificar se a situação do risco permanece estável.	<ul style="list-style-type: none"> <li>• Superintendente e/ou Equivalente</li> </ul>

**Figura 4 - Criticidade versus Controles Requeridos**


Os riscos classificados como “Alto” na Matriz de Avaliação de Riscos deverão ser apresentados formalmente pela área de GRIC ao Diretor da área e ao Presidente da Empresa.

Os riscos classificados como “Alto” e que têm impacto direto no atingimento dos objetivos estratégicos devem ser reportados à DE e ao CA.

Os riscos com impacto na continuidade do negócio devem possuir plano de contingência proposto e aprovado pela Diretoria e submetido para a ciência do CA.

A avaliação deve subsidiar as respostas aos riscos, que podem ser:

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 12 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- **Eliminar:** implica em evitar os riscos, eliminando a causa do evento do risco ou modificando a atividade e processo de modo a resguardar seus objetivos contra tais eventos;
- **Mitigar:** adoção de medidas para reduzir a probabilidade ou o impacto dos riscos aos níveis aceitáveis definidos pela DE;
- **Compartilhar / Transferir:** redução da responsabilidade ou do impacto pela transferência ou pelo compartilhamento do risco com um terceiro;
- **Aceitar:** nenhuma medida será adotada para afetar a probabilidade ou o grau de impacto dos riscos, considerando uma decisão consciente de assumir o risco.

### Critérios de Aceitação de Riscos


Os critérios de Aceitação de Riscos representam a tolerância dos riscos que a Empresa está disposta a aceitar, de acordo com o Apetite ao Risco que a Diretoria Executiva estipular.

A tabela abaixo apresenta as categorias de risco e seus respectivos critérios para aceitação.

**Tabela 4 - Critérios de Aceitação dos Riscos**

<b>Categoria do Risco</b>	<b>Critério de Aceitação</b>
Estratégico	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
De Imagem	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
De Pessoas	Serão aceitos quando não houver pessoas para recolocação, impossibilidade de mudança de processos, de redefinição de prioridades ou de processos.
Operacional	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
Financeiro/Orçamentário	Só serão aceitos quando não houver formas alternativas de financiamento, de corte de gastos, nem de renegociação.
De Tecnologia da Informação	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
De Integridade	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
Legal	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 13 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

De Riscos do Meio Ambiente	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.
De Segurança da Informação	Os riscos devem ser mitigados, evitados ou transferidos, pois não poderão ser aceitos.

### Tratamento dos riscos

Para o tratamento dos riscos devem ser estabelecidos planos de ação e executadas medidas de controle com a finalidade de alterar o nível de criticidade, tornando-o compatível com o apetite ao risco da EPE, definido pela Diretoria Executiva.

O tratamento proposto deve contemplar a análise de custo-benefício, sempre que possível.

Os controles aplicados devem ser formalmente estabelecidos e documentados, sendo acompanhados por meio de registros e indicadores, quantitativos e/ou qualitativos.

### Monitoramento e Análise Crítica

O processo contínuo de verificação, supervisão, observação crítica ou identificação da situação comportamental dos eventos críticos será conduzido pela GRIC por meio do recebimento dos documentos e relatórios gerados pelos responsáveis pelo risco com periodicidade mensal.

Os resultados do monitoramento deverão ser registrados e comunicados para os gestores e respectivos Diretores/Presidente.

A adoção de indicadores tem o objetivo de mensurar os resultados das tarefas e o monitoramento de desempenho de práticas adotadas para a gestão dos riscos. Todo projeto deve ter indicadores de gestão de risco criados por seus respectivos responsáveis.

### Comunicação e Consulta

A comunicação do risco e a consulta às partes internas e externas devem acontecer durante todas as fases do processo de gestão de riscos e a qualquer momento. Essa comunicação deverá ser munida com o preenchimento da tabela de matriz de riscos.

A área responsável por receber essas demandas é o Comitê Executivo de Governança, Riscos e Controles Internos (CGRIC-X), e deve ser representado pelo responsável da área onde o risco está se manifestando.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 14 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

O monitoramento será feito pelo Gestor de Riscos, cujo resultado será documentado pelo mesmo e repassado bimestralmente à Diretoria Executiva da EPE.

## 5.2. Controles Internos da Gestão

Compreende o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de empregados da Empresa, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão institucional, os seguintes objetivos gerais serão alcançados:

- a) execução ordenada, ética, econômica, eficiente e eficaz das operações;
- b) cumprimento das obrigações de accountability;
- c) cumprimento das leis e regulamentos aplicáveis;
- d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados de forma eficaz, eficiente, efetiva e econômica;
- e) a gestão de eventos ou condições de incerteza que, se ocorrerem, acarretarão em um efeito negativo sobre um ou mais objetivos planejados pela Empresa.

### 5.2.1. Papéis e Responsabilidades

#### Conselho de Administração

Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a EPE,

#### Diretoria Executiva

Estabelecer, manter, monitorar e aperfeiçoar os controles internos da gestão, sem prejuízo das responsabilidades dos gestores dos processos organizacionais e de programas de governos nos seus respectivos âmbitos de atuação.

#### Empregados

Operacionalizar os controles internos da gestão e identificar e comunicar deficiências às instâncias superiores, de acordo com o documento em anexo “Procedimento Metodológico de Gestão de Controles Internos.”

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 15 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

## 5.2.2. Detalhamento


A EPE deve implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos para o negócio. Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa da Empresa, para propiciar o alcance de seus objetivos.

Esses controles deverão ser operados por todos os empregados responsáveis pela condução das suas atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio da Empresa. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos da Empresa. Assim, tendo em vista os objetivos estabelecidos, e os riscos decorrentes de eventos internos ou externos que possam obstaculizar o alcance desses objetivos, devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto sobre os objetivos organizacionais.

- Os controles internos da gestão devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas.
- Os controles internos da gestão baseiam-se no gerenciamento de riscos e integram o processo de gestão.
- Os componentes dos controles internos da gestão e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências da Empresa.
- A DE da EPE deve assegurar que procedimentos efetivos de implementação de controles internos da gestão façam parte de suas práticas de gerenciamento de riscos.
- Controles internos da gestão adequados devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão da EPE.
- Os controles internos da gestão devem integrar as atividades, planos, ações, políticas, sistemas, recursos e esforços de todos que trabalhem na EPE, sendo projetados para fornecer segurança razoável de que a EPE atingirá seus objetivos e missão.
- Os controles internos da gestão não devem ser implementados de forma circunstancial, mas como uma série de ações que permeiam as atividades da Empresa. Essas ações se dão em todas as operações da EPE de modo contínuo, inerentes à maneira pela qual o gestor administra a sua área de atuação.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 16 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	



	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- São instâncias de segunda linha (ou camada) de defesa, para supervisão e monitoramento dos controles internos: o Comitê Executivo de Governança, Riscos, Integridade e Controles Internos, assim como a área de Governança, Riscos, Integridade e Controles Internos.
- Os controles internos da gestão tratados nesta norma não devem ser confundidos com as atividades do Sistema de Controle Interno relacionadas no artigo 74 da Constituição federal de 1988, nem com as atribuições da auditoria interna.

### 5.2.2. Princípios

Os controles internos da gestão da EPE devem ser desenhados e implementados em consonância com os seguintes princípios:

- I - aderência à integridade e a valores éticos;
- II - competência da alta administração em exercer a supervisão do desenvolvimento e do desempenho dos controles internos da gestão;
- III - coerência e harmonização da estrutura de competências e responsabilidades dos diversos níveis de gestão da Empresa;
- IV - compromisso da alta administração em atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos da EPE;
- V - clara definição dos responsáveis pelos diversos controles internos da gestão no âmbito da organização;
- VI - clara definição de objetivos que possibilitem o eficaz gerenciamento de riscos;
- VII - mapeamento das vulnerabilidades que impactam os objetivos, de forma que sejam adequadamente identificados os riscos a serem geridos;
- VIII - identificação e avaliação das mudanças internas e externas à Empresa que possam afetar significativamente os controles internos da gestão;
- IX - desenvolvimento e implementação de atividades de controle que contribuam para a obtenção de níveis aceitáveis de riscos;
- X - adequado suporte de tecnologia da informação para apoiar a implementação dos controles internos da gestão;
- XI - definição de políticas e normas que suportem as atividades de controles internos da gestão;
- XII - utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão;

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 17 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	<b>NORMA Nº</b> <b>NOG-GRIC-017</b>	
		<b>VERSÃO</b>	<b>APROVADO EM</b>
		01	09/04/2018

- XIII - disseminação de informações necessárias ao fortalecimento da cultura e da valorização dos controles internos da gestão;
- XIV - realização de avaliações periódicas para verificar a eficácia do funcionamento dos controles internos da gestão; e
- XV - comunicação do resultado da avaliação dos controles internos da gestão aos responsáveis pela adoção de ações corretivas, incluindo a alta administração.

### 5.2.3. Dos Objetivos dos Controles Internos da Gestão

Os controles internos da gestão devem ser estruturados para oferecer segurança razoável de que os objetivos da Empresa sejam alcançados. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos da gestão.

Dessa forma, a área de Governança, Riscos, Integridade e Controles Internos deve:

- I - Verificar a eficiência<sup>1</sup>, a eficácia<sup>2</sup> e a efetividade<sup>3</sup> operacional, analisando se as operações estão sendo executadas de forma ordenada, com ética<sup>4</sup> e economicidade<sup>5</sup>;
- II - Verificar se as informações produzidas são íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas;
- III - Verificar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria EPE, de acordo com a metodologia do documento em anexo. Para tal, fica instituído o “**Procedimento Metodológico de Gestão de Controles Internos**”, documento em anexo a essa norma, de forma a se viabilizar e operacionalizar a análise de conformidade ; e
- IV - Salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

<sup>1</sup> As operações da EPE serão eficientes quando consumirem o mínimo de recursos para alcançar uma dada quantidade e qualidade de resultados, ou alcançarem o máximo de resultado com uma dada qualidade e quantidade de recursos empregados.

<sup>2</sup> As operações da EPE serão eficazes quando cumprirem objetivos imediatos, traduzidos em metas de produção ou de atendimento, de acordo com o estabelecido no planejamento das ações.

<sup>3</sup> As operações da EPE serão efetivas quando alcançarem os resultados pretendidos a médio e longo prazo, produzindo impacto positivo e resultando no cumprimento dos objetivos das organizações.

<sup>4</sup> Ética se refere aos princípios morais, sendo pré-requisito e suporte para a confiança pública.

<sup>5</sup> As operações da EPE serão econômicas quando a aquisição dos insumos necessários se der na quantidade e qualidade adequadas, forem entregues no lugar certo e no momento preciso, ao custo mais baixo.

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 18 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

#### 5.2.4. Da Estrutura dos Controles Internos da Gestão

Na implementação dos controles internos da gestão, a alta administração, bem como os empregados da EPE, devem observar os seguintes componentes da estrutura de controles internos:

I - ambiente de controle: é a base de todos os controles internos da gestão, sendo formado pelo conjunto de regras e estrutura que determinam a qualidade dos controles internos da gestão. O ambiente de controle deve influenciar a forma pela qual se estabelecem as estratégias e os objetivos e na maneira como os procedimentos de controle interno são estruturados. Alguns dos elementos do ambiente de controle são:

- a) integridade pessoal e profissional e valores éticos assumidos pela direção e pelo quadro de empregados, incluindo inequívoca atitude de apoio à manutenção de adequados controles internos da gestão, durante todo o tempo e por toda a organização;
- b) comprometimento para reunir, desenvolver e manter colaboradores competentes;
- c) filosofia da direção e estilo gerencial, com clara assunção da responsabilidade de supervisionar os controles internos da gestão;
- d) estrutura organizacional na qual estejam claramente atribuídas responsabilidades e delegação de autoridade, para que sejam alcançados os objetivos da organização ou das políticas públicas; e
- e) políticas e práticas de recursos humanos, especialmente a avaliação do desempenho e prestação de contas dos colaboradores pelas suas responsabilidades pelos controles internos da gestão da organização ou política pública.

II - **avaliação de risco**: é o processo permanente de identificação e análise dos riscos relevantes que impactam o alcance dos objetivos da organização e determina a resposta apropriada ao risco.

Envolve identificação, avaliação e resposta aos riscos, devendo ser um processo permanente;

III - **atividades de controles internos**: são atividades materiais e formais, como políticas, procedimentos, técnicas e ferramentas, implementadas pela gestão para diminuir os riscos e assegurar o alcance de objetivos organizacionais e de políticas públicas. Essas atividades podem ser preventivas (reduzem a ocorrência de eventos de risco) ou detectivas (possibilitam a identificação da ocorrência dos eventos de risco), implementadas de forma manual ou automatizada. As atividades de controles internos devem ser apropriadas, funcionar consistentemente de acordo com um plano de longo prazo, ter custo adequado, ser abrangentes, razoáveis e diretamente relacionadas aos objetivos de controle. São exemplos de atividades de controles internos:

- a) procedimentos de autorização e aprovação;

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 19 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

b) segregação de funções (autorização, execução, registro, controle);

c) controles de acesso a recursos e registros;

d) verificações;

e) conciliações;

f) avaliação de desempenho operacional;

g) avaliação das operações, dos processos e das atividades; e

h) supervisão.


IV - **informação e comunicação**: as informações produzidas pela EPE devem ser apropriadas, tempestivas, atuais, precisas e acessíveis, devendo ser identificadas, armazenadas e comunicadas de forma que, em determinado prazo, permitam que nossos funcionários e servidores cumpram suas responsabilidades, inclusive a de execução dos procedimentos de controle interno. A comunicação eficaz deve fluir para baixo, para cima e através da organização, por todos seus componentes e pela estrutura inteira. Todos os funcionários devem receber mensagem clara da alta administração sobre as responsabilidades de cada agente no que concerne aos controles internos da gestão. A organização deve comunicar as informações necessárias ao alcance dos seus objetivos para todas as partes interessadas, independentemente no nível hierárquico em que se encontram;

V - **monitoramento**: é obtido, por meio de revisões específicas ou monitoramento contínuo, independente ou não, realizado sobre todos os demais componentes de controles internos, com o fim de aferir sua eficácia, eficiência, efetividade, economicidade, excelência ou execução na implementação dos seus componentes e corrigir tempestivamente as deficiências dos controles internos:

a) **monitoramento contínuo**: é realizado nas operações normais e de natureza contínua da EPE. Inclui a administração e as atividades de supervisão e outras ações que os funcionários executam ao cumprir suas responsabilidades. Abrange cada um dos componentes da estrutura do controle interno, fortalecendo os controles internos da gestão contra ações irregulares, antiéticas, antieconômicas, ineficientes e ineficazes. Pode ser realizado pela própria Administração por intermédio de instâncias de conformidade, como comitês específicos, que atuam como segunda linha (ou camada) de defesa da organização; e

b) **avaliações específicas**: são realizadas com base em métodos e procedimentos predefinidos, cuja abrangência e frequência dependerão da avaliação de risco e da eficácia dos procedimentos de monitoramento contínuo. Abrangem, também, a avaliação realizada pelas unidades de auditoria interna

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 20 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	

 Empresa de Pesquisa Energética	<b>NORMA DE GESTÃO DE RISCOS E DE CONTROLES</b>  <b>INTERNOS</b>	NORMA Nº NOG-GRIC-017	
		VERSÃO	APROVADO EM
		01	09/04/2018

dos órgãos e entidades e pelos órgãos do Sistema de Controle Interno (SCI) do Poder Executivo federal para aferição da eficácia dos controles internos da gestão quanto ao alcance dos resultados desejados.

Os componentes de controles internos da gestão definem o enfoque recomendável para a estrutura de controles internos nos órgãos e entidades do setor público e fornecem bases para sua avaliação. Esses componentes se aplicam a todos os aspectos operacionais de cada organização.

## 6. Disposições Gerais

Casos omissos ou excepcionais serão submetidos à aprovação da Diretoria Executiva.

A não observância aos dispositivos dessa norma pode acarretar, nos termos da legislação aplicável, sanções administrativas, civis e/ou penais.

## 7. Anexos

*A partir desse momento fica instituída o “Procedimento Metodológico de Gestão de Riscos” e o “Procedimento Metodológico de Gestão de Controles Internos”, ambos anexos a essa norma.*

***Este Instrumento Normativo entra em vigor em 09/04/2018 conforme decisão da Diretoria Executiva da EPE.***

ELABORADO POR	DOCUMENTO DE APROVAÇÃO	Página 21 de 21
PR/EPE	RD nº 01/450 <sup>a</sup>	