 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

## Sumário

1. OBJETIVO .....	2
2. ÂMBITO DE APLICAÇÃO .....	2
3. DEFINIÇÕES .....	2
4. DOCUMENTOS DE REFERÊNCIAS .....	5
5. RESPONSABILIDADES .....	5
6. REGRAS BÁSICAS .....	5
7. CONTROLE DE REGISTROS .....	11
8. ANEXOS .....	11
9. REGISTRO DE ALTERAÇÕES .....	12

### 1. OBJETIVO

Estabelecer critérios para a elaboração da matriz de risco dos processos e priorização dos trabalhos a serem incluídos no Plano Anual de Auditoria.

### 2. ÂMBITO DE APLICAÇÃO

#### 2.1. Empresa

Aplica-se em todas as Empresas do Grupo CPFL.

#### 2.2. Área


Gerência de Auditoria Interna

### 3. DEFINIÇÕES

#### 3.1. AUDITORIA INTERNA

Auditoria Interna é uma atividade independente e objetiva que presta serviços de avaliação (assurance) e de consultoria e tem como objetivo adicionar valor e melhorar as operações de uma organização. A Auditoria auxilia a organização a alcançar seus objetivos adotando uma abordagem sistemática e disciplinada para a avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, de controle, e governança corporativa. *(Fonte: IIA – Normas Internacionais para o Exercício Profissional de Auditoria Interna)*

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	2 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

### 3.2. COMITÊ DE AUDITORIA INTERNA

O Comitê de Auditoria (CoAud) é órgão permanente da Companhia, de assessoramento do Conselho de Administração ("CA"), com dotação orçamentária própria, para conduzir ou determinar a realização de consultas, avaliações e investigações dentro do escopo de suas atividades, incluindo a contratação de advogados e especialistas externos, dentro dos limites aprovados pelo CA conforme solicitado pelo próprio CoAud.

O CoAud atuará com autonomia e independência no exercício de suas funções, reportando-se diretamente ao CA e servindo como órgão auxiliar, consultivo e de assessoramento, sem poder decisório ou atribuições executivas.

### 3.3. CONFORMIDADE

No âmbito institucional e corporativo, conformidade é o conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da empresa, bem como evitar, detectar e tratar qualquer desvio ou falta de aderência que possa ocorrer.

### 3.4. CONTROLE INTERNO


Conjunto de processos, incluindo políticas, procedimentos, práticas e estruturas organizacionais utilizados na atividade de alinhamento periódico da estrutura de controles da organização em relação aos riscos (internos e externos) inerentes às suas atividades. Controle Interno adequado é aquele resultante de estruturas e sistemas capazes de propiciar uma razoável margem de garantia de que os objetivos e metas da organização serão atingidos de maneira eficaz, eficiente e com a necessária economicidade.

### 3.5. COSO

O *Committee of Sponsoring Organizations of the Treadway Commission* – COSO é uma organização voluntária do setor privado dedicada a aprimorar a qualidade dos reportes financeiros como resultado de negócios éticos, controles internos efetivos e governança corporativa. Formada em 1985 para patrocinar a National Commission on Fraudulent Financial Reporting, estudou os principais fatores que causam fraudes nas demonstrações financeiras e desenvolveu recomendações para companhias, seus auditores e para a SEC (Securities Exchange Commission).

Patrocinada pelas cinco maiores associações de profissionais ligados à área financeira dos Estados Unidos (AAA - American Accounting Association, AICPA - American

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	3 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

*Institute of Certified Public Accountants, FEI -Financial Executives Institute, IIA Institute of Internal Auditors e IMA -Institute of Management Accountants), contém representantes da indústria, firmas de auditoria, firmas de investimento e da Bolsa de Valores de Nova Iorque.*

### 3.6. INSTITUTO DOS AUDITORES INTERNOS – IIA

Fundado em 1960, o IIA Brasil – Instituto dos Auditores Internos do Brasil é uma entidade civil, sem fins lucrativos, constituída por pessoas físicas que atuam em atividades de Auditoria Interna. O Instituto representa a comunidade nacional de auditores internos e dos profissionais de controle interno e externo e tem como objetivo principal o fortalecimento da categoria, sua formação, capacitação e atualização. Filiado ao The Institute of Internal Auditors – IIA, o IIA Brasil realiza cursos, reuniões e eventos para debater o assunto Auditoria Interna. A entidade também atua para difundir o reconhecimento e a importância da função do auditor interno no âmbito dos setores privado e público. (www.iiabrasil.org.br)

### 3.7. MATRIZ DE RISCO

Metodologia que consiste na classificação dos processos auditáveis através da ponderação de diversos indicadores de risco, com pontuações variáveis, objetivando uma definição mais adequada das prioridades de exames dentro da Empresa, de forma a reduzir os inconvenientes efeitos do subjetivismo.


A Matriz de Risco apresenta de forma mais objetiva quais os exames deveriam ser prioritariamente realizados pela Auditoria Interna, porém, razões de ordem administrativa ou estratégica poderão determinar alterações nas prioridades definidas.

### 3.8. PADRÕES E INDICADORES DE RISCO

Os indicadores de risco são os elementos utilizados pela Auditoria Interna para definição das prioridades de exames. Os padrões de indicadores utilizados pela Auditoria Interna são baseados no pronunciamento do Instituto dos Auditores Internos (IIA) e conceitos do COSO e consideram 6 (seis) fatores para categorizar o “**impacto**” de materialização do risco, são estes: Estratégico, Operacional, Saúde e Segurança, Legal/Regulatório, Reputacional e Financeiro, e 6 (seis) fatores para categorizar a “**vulnerabilidade**” (probabilidade) na qual a Companhia possa estar exposta: sendo estes: Sistemas e Segurança de Informação, Rotação de Ênfase, Resposta aos Riscos e Controles Internos, Gestão de Continuidade, Percepções e Entrevistas e Condições Externas.

Para cada indicador de risco é definido um fator de relevância correspondente em função de sua relevância no processo. Os fatores variam de 1 a 4, sendo 1 indicativo

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	4 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

de **Baixa Relevância** e **4** indicativos de **Alta Relevância**. Para alguns critérios estabelecemos também a possibilidade de não se aplicar, ou seja, N/A.

### 3.9. PLANO ANUAL DE AUDITORIA INTERNA

Documento contendo os projetos e ações a serem desenvolvidos pela Auditoria Interna durante o ano, considerando a importância estratégica dos processos, análise dos riscos, carga horária disponível do staff de auditores e previsões de duração de cada trabalho.

### 3.10. RISCO

A incerteza de um evento superveniente que possa ter impacto na consecução dos objetivos. O risco é medido em termos de impacto e probabilidade.

## 4. DOCUMENTOS DE REFERÊNCIAS

Procedimento GED nº 05614 – Modelo de Maturidade dos Processos  
 Procedimento GED nº 13134 – Normas Internacionais de Auditoria  
 Procedimento GED nº 13135 – Regulamento da Auditoria Interna

## 5. RESPONSABILIDADES

Compete à Auditoria Interna a definição das prioridades de trabalhos a serem incluídos no Plano Anual de Auditoria.

Compete ao Comitê de Auditoria revisão do material produzido pela Auditoria para suporte do Plano Anual de Auditoria e sua recomendação para aprovação pelo Conselho de Administração.

Compete ao Conselho de Administração a aprovação final do plano anual de auditoria.


## 6. REGRAS BÁSICAS

### 6.1. ELABORAÇÃO DO PLANO ANUAL DE AUDITORIA INTERNA

A partir do segundo semestre de cada ano os Gestores da Auditoria Interna se reunirão para iniciar as atividades envolvendo a análise dos dados e preparo da documentação necessária à elaboração do Plano Anual de Trabalhos do ano seguinte.

A elaboração do Plano Anual de Auditoria será realizada de acordo com as técnicas de gerenciamento de riscos e deverá considerar:

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	5 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

- Entrevistas com os executivos da CPFL Energia a fim de obter as principais preocupações e áreas de ênfase no contexto da Auditoria Interna;
- Obtenção da percepção e expectativas do Conselho Fiscal e do Comitê de Auditoria Interna com relação aos processos a serem auditados;
- Sinergia com os trabalhos realizados pela Gestão de Riscos e Compliance para a identificação e avaliação dos indicadores de potenciais de riscos (estratégicos, financeiros, operacionais e regulamentares), considerando aspectos de controle, gestão e tecnologia;
- Revisão e atualização da classificação dos riscos e do Mapa e Dicionário de Riscos;
- Reavaliação e alocação dos riscos corporativos por processo e empresa do Grupo, suportado pelos critérios do Instituto dos Auditores Internos (IIA) e COSO;
- Avaliação da criticidade dos processos de negócio e de apoio de acordo com a vulnerabilidade e impacto envolvidos;
- Estabelecimento de um plano anual de trabalhos da Auditoria Interna para todas as empresas da Companhia, considerando os riscos e processos mais críticos.

O Plano Anual de Auditoria será submetido à apreciação do Comitê de Auditoria. Este deverá recomendar sua aprovação ao Conselho de Administração. Após a aprovação pelo Conselho de Administração, o Plano de Auditoria será levado ao conhecimento da Presidência e Vice-presidências.


Qualquer alteração, substituição ou postergação de trabalhos previstos no plano somente poderá ser feita com a aprovação do responsável pela Auditoria Interna que deverá levar o fato e justificativas ao Comitê de Auditoria Interna e ao Conselho de Administração.

## 6.2. CLASSIFICAÇÃO DOS PROCESSOS POR CRITICIDADE

A Classificação da Criticidade dos Processos é utilizada para documentar e categorizar os principais processos da Companhia e dessa forma desenvolver um entendimento padronizado do Universo da Auditoria Interna.

Na sua elaboração os macroprocessos, processos e subprocessos existentes no Grupo CPFL devem ser alinhados e endereçados de acordo com as características e particularidades do segmento de negócio (Geração, Distribuição, Comercialização, Serviços, Telecomunicações e Transmissão) ou de apoio (atividades corporativas).

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	6 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

A avaliação e classificação dos processos a serem auditados é feita pela Auditoria Interna de forma independente, ou seja, sem qualquer pressão de qualquer órgão da administração. No entanto, a Auditoria Interna utiliza o resultado do trabalho de análise de riscos produzido pela mesma à época da elaboração do plano. Além disso, devem ser utilizados os principais padrões e indicadores de avaliação de riscos do pronunciamento do Instituto dos Auditores Internos (IIA).

O modelo adotado pela Auditoria Interna da CPFL considera os seguintes fatores:

**IMPACTO:**

- ✓ Legal / Regulatório
- ✓ Estratégico
- ✓ Operacional
- ✓ Saúde e Segurança
- ✓ Financeiro
- ✓ Reputacional

**VULNERABILIDADE:**

- ✓ Resposta aos Riscos
- ✓ Controles Internos
- ✓ Condições Externas
- ✓ Gestão de Continuidade
- ✓ Percepções e Entrevistas
- ✓ Sistemas e Segurança da Informação

### 6.3. CÁLCULO DA CRITICIDADE DOS PROCESSOS

Os cálculos de criticidade de cada processo serão elaborados de conformidade com os fatores e parâmetros a seguir:

**Fator: IMPACTO**


**Estratégico:** Está ligado à qualidade dos aspectos de controle interno e organizacionais existentes no ambiente em que as operações se processam. Está ligado ao alcance dos objetivos estratégicos:

- 1 - Mínima;
- 2 - Pequena;
- 3 - Moderada;
- 4 - Forte;
- N/A - Não se Aplica.

**Operacional:** Envolve aspectos e impactos operacionais relacionados a natureza do processo. A análise deve considerar a possibilidade de eventos críticos bem como os esforços internos para mitigar os impactos na organização:

- 1 - Mínima;
- 2 - Pequena;
- 3 - Moderada;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	7 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

4 - Forte;  
N/A - Não se Aplica.

**Saúde e Segurança:** Visa identificar o grau de impacto dos fatores de saúde e segurança no processo:

1 - Mínima;  
2 - Pequena;  
3 - Moderada;  
4 - Forte;  
N/A - Não se Aplica.

**Legal / Regulatório:** Visa identificar o grau de impacto da legislação e/ou regulação (compliance) nas operações da empresa ou processo a ser auditado:

1 - Mínima;  
2 - Pequena;  
3 - Moderada;  
4 - Forte;  
N/A - Não se Aplica.


**Reputacional:** Envolve aspectos relacionados ao comprometimento da imagem interna ou externa da Empresa:

1 - Público Interno;  
2 - Clamor da Mídia Local;  
3 - Clamor da Mídia Estadual;  
4 - Clamor da Mídia Nacional / Internacional;  
N/A - Não se Aplica.

**Financeiro:** Trata da relevância do valor, do volume de recursos envolvidos, do tamanho dos ativos, ou do volume de transações; entre outros aspectos, isoladamente ou em determinado processo ou contexto:

1 - Até 5%;  
2 - Até 15%;  
3 - Até 30%;  
4 - Maior que 30%;  
N/A - Não se Aplica.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	8 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

### Fator: Vulnerabilidade

**Sistemas e Segurança da Informação:** Envolve aspectos de qualidade dos sistemas e nível de automação do processo. Envolve, também, as condições de segurança das informações inerentes ao processo:

- 1 - Integrado;
- 2 - Automático;
- 3 - Digital;
- 4 - Manual;
- N/A - Não se Aplica.

**Resposta aos Riscos e Controles Internos:** Indica o comportamento da empresa em relação aos insumos coletados das análises de gestão de riscos e controles internos:

- 1 - Excelente;
- 2 - Satisfatória;
- 3 - Regular;
- 4 - Insuficiente;
- N/A - Não se Aplica.

**Gestão de Continuidade:** Indica o comportamento da empresa em relação a mudanças organizacionais, operacionais, tecnológicas, segurança, qualidade, treinamento, gestão, resultados e continuidade:


- 1 - Imediata;
- 2 - Rápida;
- 3 - Lenta;
- 4 - Inerte;
- N/A - Não se Aplica.

**Percepções e Entrevistas:** Envolve as percepções e preocupações da alta gestão:

- 1 – Processo não mencionado;
- 2 - Preocupações dos Gerentes e Coordenadores;
- 3 – Preocupações dos Diretores e VPs;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	9 de 12



 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

4 – Preocupações dos Comitês, Conselhos e acionistas;  
 N/A - Não se Aplica.

**Condições Externas:** Indica o comportamento da empresa em relação a competitividade, tendências de mercado e condições adversas como racionamento ou hidrologia desfavorável:

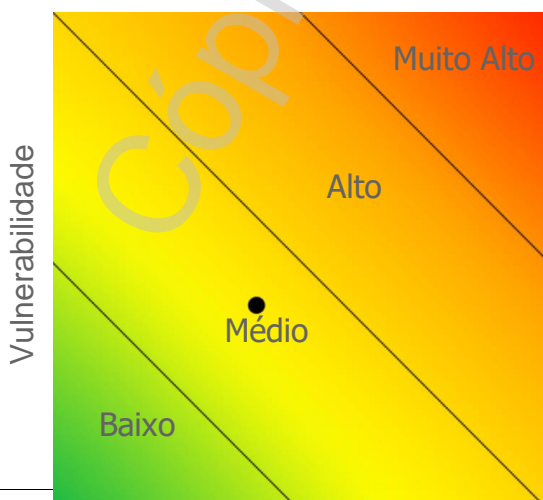
1 - Excelente;  
 2 - Satisfatório;  
 3 - Regular;  
 4 - Insuficiente;  
 N/A - Não se Aplica.

#### 6.4.PRIORIZAÇÃO DOS TRABALHOS A SEREM INCLUÍDOS NO PLANO


A relevância de cada um desses fatores, vulnerabilidade e impacto é calculada pela média da soma da pontuação dos parâmetros atribuídos.

A priorização dos trabalhos de auditoria é definida a partir da intersecção do valor médio atribuído aos 6 (seis) fatores de “**IMPACTO**” do processo (Eixo das Abscissas), com a média dos valores atribuídos aos 5 (cinco) fatores de “**VULNERABILIDADE**” – Eixo das Ordenadas).

A prioridade é dada de acordo com o gradiente do gráfico de risco em que o processo se encontrar, conforme segue (imagem ilustrativa):



N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	10 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

Todos os processos com classificação final Muito Alto e Alto serão selecionados para avaliação no Plano Anual de Auditoria.

#### 6.4.1 ROTAÇÃO DE ÊNFASE

Processos classificados como média e baixa criticidade serão auditados em ciclos de 2 (dois) à 5 (cinco) anos, dependendo da relevância do assunto. Para tal será aplicada a rotação de ênfase, que consiste na análise dos planos de trabalho dos anos anteriores buscando verificar o último ano de análise do processo classificado.

#### 7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
N/A	N/A	N/A	N/A	N/A	N/A


#### 8. ANEXOS

ANEXO I - Modelo de Classificação da Criticidade dos Processos

##### ANEXO I

##### Modelo de Classificação da Criticidade dos Processos

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	11 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria



## 9. REGISTRO DE ALTERAÇÕES


### 9.1. Colaboradores

Empresa	Área	Nome
CPFL Paulista	Auditoria Interna	Hélio Takashi Ito
CPFL-Paulista	Auditoria Interna	Frederico Anselmo Espanholo
CPFL-Piratinga	Auditoria Interna	Geovan Carlos Mendonça Campos
CPFL-Transmissão	Auditoria Interna	Danielle Goulart Peraza Astarita

### 9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
N/A	N/A	Documento em versão inicial.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	12 de 12

 Uso Interno	Tipo de Documento: Procedimento
	Área: PAC - GERÊNCIA AUDITORIA
	Título do Documento: Matriz de Risco e Plano Anual de Auditoria

1.0	13/07/2010	Adequação ao projeto NORMA ZERO. Criação sumário, inversão de números entre "4.REFERÊNCIA" e "5.RESPONSABILIDADES", criação dos grupos "6.REGRAS BÁSICAS", "7.CONTROLES DE REGISTROS", "8.ANEXO", "9.REGISTRO DE ALTERAÇÕES", "9.1.Colaboradores" e "9.2.Alterações".
1.1	10/08/2012	Revisão conforme NORMA ZERO.
1.2	23/06/2015	Adequação por prazo de validade.
1.3	06/06/2018	Adequação por prazo de validade.
1.4	22/12/2020	Remoção do item "6.5 - ATUALIZAÇÃO DA MATRIZ DE RISCOS" e Revisão dos itens "9.REGISTRO DE ALTERAÇÕES", "9.1.Colaboradores" e "9.2.Alterações".
1.5	18/03/2022	Adequação ao projeto Revisão da Matriz de Criticidade para Avaliação dos Macroprocessos do Plano Anual de Auditoria e Revisão dos itens "3.DEFINIÇÕES", "6.REGRAS BÁSICAS", "8.ANEXO", "9.REGISTRO DE ALTERAÇÕES".

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14172	Tático	7.0	Helio Takashi Ito	29/11/2023	13 de 12