Sumário

1. OBJETIVO

Com o objetivo de prevenir o uso não autorizado, dano ou perda de informações e riscos relacionados, deve haver mecanismos de segregação de funções em sistemas e operações que suportam informações financeiras da empresa para evitar fraudes e perdas.
Este documento tem por finalidade estabelecer os mecanismos de revisão periódica dos riscos, transações críticas e conflitantes e de controles compensatórios, contidas nas Matrizes de Segregações de Funções dos sistemas dos ambientes (SAP ECC, SAP CCS). Para os ambientes Non SAP, consultar a GED 19270 - Procedimento de Revisão das Matrizes de Segregação SOD Non-SAP.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas do **Grupo CPFL**

2.2. Área

Todas as áreas do **Grupo CPFL** que utilizam os sistemas citados acima.

3. DEFINIÇÕES

SEGREGAÇÃO DE FUNÇÕES: Controle utilizado para prevenir e minimizar os riscos operacionais (definidos na “Matriz de Segregação de Funções”). Assegura que um único usuário não tenha acesso a duas transações conflitantes.

CONTROLE COMPENSATÓRIO: Controles desenhados para compensar de forma planejada ou deliberada uma determinada "fraqueza" do sistema de controles (detectivos ou preventivos).

Grupo CPFL: A CPFL Energia S.A., e todas as suas controladas diretas e/ou indiretas, exceto as empresas com seus próprios padrões de governança e gestão que compartilham controle com outras empresas.

4. DOCUMENTOS DE REFERÊNCIA

4.1. Internos

- Diretrizes de Segurança da Informação do **Grupo CPFL** (GED 14369);
- Código de Conduta Ética do **Grupo CPFL (**GED 19232);
- Norma para Gestão de Acessos do **Grupo CPFL** (GED 14141);
- Procedimento de Revisão das Matrizes de Segregação SOD Non-SAP (GED 19270).

4.2. Externos

- NBR ISO/IEC 27001:2013;
- Sarbanes-Oxley Act of 2002 – Section 404;
- Cobit - Control Objectives for Information and related Technology.

5. RESPONSABILIDADES

5.1. Role Owners

Revisar no tempo determinado ou, sempre que houver alteração no processo, os perfis estabelecidos, riscos envolvidos, transações críticas e/ou conflitantes contidas nas Matrizes de Segregações de Funções, caso existam divergências no perfil atribuído abrir um chamado na ferramenta disponibilizada para este fim, para regularização.

Encaminha à Diretoria de Tecnologia da Informação com as ações de ajustes/validações e as devidas providências, caso não haja ações e ajustes informados significa que os acessos serão mantidos até o próximo período de análise.

5.2. Diretoria de Tecnologia da Informação

Comunica (e orienta, se necessário) anualmente os Role Owners e Responsáveis pelos controles da necessidade de revisão e no prazo estabelecido.

Informa às áreas de negócio sobre as regras de acesso (conflitos de segregação de função/transações críticas) sempre que necessário.

Custodia a guarda das alterações informadas pelos Role Owners e apresenta para a auditoria.

5.3. Gerência de Controles Internos

Avaliar o respectivo controle compensatório (atenuação) endereçado para o conflito.

Confirmar anualmente se os respectivos controles compensatórios definidos estão válidos e avaliar a mitigação dos riscos durante a Certificação Anual de Controles Internos.

6. REGRAS BÁSICAS

6.1. Revisão Periódica dos riscos, transações críticas e conflitantes.

A Diretoria de Tecnologia da Informação anualmente comunicará as respectivas áreas de negócio, através dos respectivos Role Owners, da necessidade de revisão dos perfis existentes, transações críticas e conflitantes contidas nas Matrizes de Segregações de Funções dos sistemas do escopo Non-SAP.

Esta comunicação será através de e-mail e a revisão deverá ser realizada no período máximo de 30 dias.

Os Role Owners devem responder à Diretoria de Tecnologia da Informação através de e-mail as alterações ou manutenções dos itens nas Matrizes de Segregações de Funções.

6.2. Controles Compensatórios.

As áreas envolvidas no processo em conjunto com os Role Owners devem identificar, analisar e remediar as situações de conflitos (caso existam). Na impossibilidade de remediação, devem informar a ação mitigatória (controle compensatório) para o risco, informando a Diretoria de Tecnologia da Informação para avaliação.

A Diretoria de Tecnologia da Informação avaliará a mitigação dos riscos durante a Certificação Anual de Revisão das Matrizes de Segregações de Funções.

6.3. Revisão de Controles Compensatórios.

A Diretoria de Tecnologia da Informação anualmente solicitará às respectivas áreas de negócio, através dos respectivos responsáveis pelos controles, a confirmação dos controles compensatórios atualmente definidos.
A Gerência de Controles Internos avaliará a mitigação dos riscos durante a Certificação Anual de Controles Internos.

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
E-mail	Outlook	Backup	E-mail	Backup	Deletar

8. ANEXOS

Não aplicável.

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
CPFL Piratininga	EIQS	Heliane Pontes
CPFL Paulista	EIQS	Rafael Fedozzi

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
1	13/11/2012	Criação do Documento
1.1.	26/11/2012	Revisão do documento de acordo com as diretrizes da área de Compliance.
1.2	27/08/2013	Atualização do documento (inclusa avaliação anual da área de Compliance sobre os controles compensatórios e risco de alta criticidade)
1.3	26/11/2015	Revisão geral do documento
1.4	22/01/2016	Atualização dos sistemas
1.5	16/02/2018	Atualização dos sistemas e Gerência de Controles Internos. Reavaliação do processo para os sistemas SAP ECC e CCS.
1.6	07/06/2018	Revisão geral do documento e exceção para empresa Renováveis.
1.6	03/07/2018	Atualização dos sistemas, revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.7	24/09/2020	Revisão geral do documento e atualização do item 6.1. Revisão Periódica dos riscos, transações críticas e conflitantes.
1.8	30/06/2022	Revisão geral do documento