Sumário

1. OBJETIVO

Esta norma tem o objetivo de estabelecer regras de gestão sobre os acessos aos sistemas SAP, SAP (CRM), Mastersaf, Espaider, ZFA, EnergyIP, UtilityIQ, Ariba, Boletagem, Maxcom, Maxplan, CWSi, Logos, LogosWeb, Diretório do Servidor de Arquivo, Sage, GTS, as transações Críticas do SAP, o SAP_ALL e Função SE37 SAP ECC e GISD (EO/DM) do **Grupo CPFL**, abrangendo senhas, perfis de usuário, concessão, alteração, revogação e revisão dos acessos, bem como medidas adicionais de segurança a fim de garantir a correta utilização dos mesmos, sendo vigente para colaboradores e terceiros, que possuam acesso aos sistemas de TI.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas do **Grupo CPFL**.

2.2. Área

Todas as áreas do **Grupo CPFL**.

3. DEFINIÇÕES

Os principais termos contidos nesta norma envolvem as seguintes definições:

ÁREAS DE NEGÓCIO: todos os órgãos formais da estrutura organizacional responsáveis pela execução de processos operacionais, comerciais, técnicos, administrativos, corporativos, de novos negócios e de gestão;

ACESSO PRIVILEGIADO: São funções de administradores que possuem acesso para criar, alterar ou excluir informações dos sistemas;

CRM DYNAMICS: Ferramenta utilizada para registro das Ocorrências;

GRC: Ferramenta utilizada para registro das solicitações de acesso dos sistemas SAP/CCS e SAP/ECC, como também registra a revisão dos acessos realizada pelo Role Owner;

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.

LOG: Registro das atividades dos usuários nos sistemas;

PERFIL DE ACESSO OU FUNÇÃO: Conjunto de transações necessárias para a execução dos processos em que um usuário deve atuar em seu dia-a-dia;

PORTAL DE SERVIÇOS: Ferramenta para registro de Ocorrências no CRM Dynamics que é acessada através da intranet do **Grupo CPFL**;

REDE CORPORATIVA: Sistema de acesso ao ambiente do **Grupo CPFL** que permite o uso de recursos computacionais do grupo;

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;

SISTEMA SAP CCS: Sistema de Gestão Comercial / Faturamento das empresas CPFL Paulista, CPFL Piratininga, CPFL Jaguariúna e CPFL Santa Cruz;

SISTEMA SAP ECC/BW: Sistema de Gestão Administrativo e Financeiro (ERP) do **Grupo CPFL** e Business Intelligence / Warehouse;

SISTEMA UTILITYIQ: Sistema de Gerenciamento de Infraestrutura Avançada;

SISTEMA ZFA: Sistema utilizado para Telemedição;

USUÁRIO: Nome atribuído à pessoa que executa alguma atividade nos sistemas do **Grupo CPFL**, para a qual tem de ter um ID de identificação.

4. DOCUMENTOS DE REFERÊNCIA

Principais documentos e regulamentações relacionados com esta norma:

- Procedimento de controle de acesso à rede corporativa;
- Procedimento de controle de acesso aos Diretórios do servidor de arquivo;
- Procedimento de controle de acesso aos Sistemas SAP;
- Procedimento de revisão das Matrizes de Segregação de Funções;
- Procedimento de Controle de Acesso ao Sistema ZFA;
- Procedimento de Controle de Acesso ao Sistema UtilityIQ;
- Procedimento de Controle de Acesso ao Sistema EnergyIP;

- Procedimento de Controle de Acesso ao Sistema MasterSaf;
- Procedimento de Controle de Acesso ao Sistema CRM Dynamics;
- Procedimento de Controle de Acesso ao Sistema Espaider
- Procedimento de Controle de Acesso aos Sistemas Boletagem e Maxcom
- Procedimento de Controle de Acesso ao Sistema Maxplan
- Procedimento de Controle de Acesso ao Sistema GISD
- Procedimento de Controle de Acesso ao Sistema ARIBA
- Procedimento de Controle de Acesso ao Sistema CWSi
- Procedimento de Controle de Acesso ao Sistema Logos e LogosWeb
- Procedimento de Controle de Acesso ao Sistema Sage
- Procedimento de Controle de Acesso ao Sistema GTS
- Norma de Governança de Documentos Gerenciais
- Movimentação de Pessoal

5. RESPONSABILIDADES

5.1. A cargo do Usuário Solicitante

Preencher adequadamente os formulários no sistema CRM Dynamics ou na ferramenta GRC solicitando inclusão, criação, alteração, reset, bloqueio e desbloqueio de acesso aos sistemas corporativos necessários para a execução de suas atividades/funções diárias.

5.2. A cargo do Superior Imediato

Os Superiores Imediatos são responsáveis pelos acessos atribuídos às pessoas que prestam serviço ao órgão sob sua responsabilidade, sejam eles colaboradores das empresas do **Grupo CPFL**, contratados ou prestadores de serviço.
Tem como responsabilidade avaliar as solicitações e os riscos de segregação de funções, e com base nesta avaliação, aprovar ou reprovar formalmente através do CRM Dynamics ou ferramenta GRC, as solicitações encaminhadas pelo usuário solicitante, e quando houver riscos de segregação, caberá também propor o controle compensatório a ser implementado visando mitigar os riscos identificados.
Excluir os acessos do colaborador sem vínculo empregatício, quando do encerramento de suas atividades/funções na área ou quando do término do contrato de Prestação de Serviços, sob sua responsabilidade.

5.3. A cargo dos Responsáveis indicados pela revisão de acesso

Revisar os usuários com acesso ao sistema e seus respectivos perfis.
Caso existam divergências no acesso abrir um chamado, na ferramenta disponibilizada para este fim, para regularização.

5.4. A cargo da Diretoria de Tecnologia da Informação

Analisar e executar a solicitação aprovada, obedecendo às regras de negócio e aos critérios de Segregação de funções estabelecidos.
Desenvolver novos perfis e realizar manutenção nos perfis existentes, mediante solicitações aprovadas.
Informar o status das solicitações e comunicar trimestralmente os responsáveis indicados da responsabilidade pela revisão dos acessos e disponibilizar, quando necessário, os relatórios de usuários com acesso aos sistemas.

Acompanhar a execução das revisões de acesso realizadas pelas áreas de negócio, reportar aos respectivos diretores à não execução e excluir o acesso, dos responsáveis da rede caso a revisão não seja realizada.

5.5. A cargo da Gerência de Serviços de RH

Manter atualizado o cadastro dos funcionários quanto às movimentações do quadro de pessoal (transferências, desligamentos e admissões, afastamentos, férias e licenças de diversas naturezas). Informar os desligamentos de colaboradores com vínculo empregatício com as empresas do **Grupo CPFL** para a exclusão dos acessos destes colaboradores nos sistemas de TI.

6. REGRAS BÁSICAS

6.1. Concessão, alteração e revogação de acessos.

Todas as solicitações para concessão, alteração ou revogação de acessos devem ser realizadas através do CRM Dynamics, salvo os sistemas SAP, que são realizadas na ferramenta GRC.

Somente os colaboradores designados pela Diretoria de Tecnologia da Informação deverão ter acesso às transações para criar, excluir, bloquear, desbloquear e reiniciar conta de usuário, bem como atribuir ou excluir perfis de acesso no ambiente produtivo.

A solicitação de concessão, alteração, exclusão, bloqueio e desbloqueio ou criação de perfis de acessos para o colaborador ter acesso aos sistemas corporativos, deve ser aprovada pelo superior imediato ou substituto autorizado do colaborador.

Os acessos devem ser liberados respeitando-se os critérios de segregação de funções.

Criação de perfis de acesso deve ser executada no ambiente de desenvolvimento e transportada para produção. A criação de acesso para novos usuários está condicionada à disponibilidade de licenças contratadas.

Os acessos aos sistemas corporativos para terceiros devem ser concedidos apenas quando a data de expiração do contrato de prestação de serviços firmado com as empresas do **Grupo CPFL** seja informada no chamado.

Na ausência desta informação o acesso não será concedido e o chamado será rejeitado.

Quando da concessão do acesso ou do reset de senha, o colaborador receberá uma senha criada pela área de Tecnologia da Informação, a qual deverá ser substituída no primeiro acesso ao sistema corporativo solicitado.

Quando da transferência de colaboradores devem seguir a norma de Movimentação de Pessoal (GED 17038).

Quando as atribuições e/ou atividades executadas por um colaborador sofrerem mudanças, o Gestor deve solicitar o cancelamento dos acessos que não serão mais necessários e a inclusão das novas necessidades de acesso.

Quando do desligamento de colaboradores com vínculo empregatício com as empresas do **Grupo CPFL**, a Gerência de Serviços de RH deverá comunicar o fato à Diretoria de Tecnologia da Informação imediatamente para que seus acessos sejam cancelados.

Quando do desligamento de colaboradores sem vínculo empregatício com as empresas do **Grupo CPFL**, o superior imediato do contrato de prestação de serviço deverá abrir chamado no CRM Dynamics ou na ferramenta GRC solicitando o cancelamento dos acessos.

6.2. Identificação dos usuários e privilégios de acesso

A identificação do usuário aos sistemas corporativos é pessoal e intransferível, e o colaborador é responsável por seu uso segundo as políticas e diretrizes vigentes. A “identificação do usuário” (código “usuário”) deve ser padronizada, única, não reutilizável, e acompanhá-lo enquanto estiver vinculada ao **Grupo CPFL**.

Os técnicos da Diretoria de Tecnologia da Informação que, em função da natureza de suas atribuições, necessitarem de acessos às transações específicas de criação ou modificação no ambiente produtivo, poderão ter sua utilização liberada, desde que justificados e autorizados pelo Gestor de TI responsável pelo sistema solicitado.

O uso de acesso privilegiado e irrestrito aos dados de produção é restrito e será monitorado pontualmente pela Diretoria de Tecnologia da Informação.

6.3. Identificação dos Usuários Privilegiados

Todo e qualquer usuário privilegiado somente poderá ser criado após aprovação pelo gestor da Diretoria de Tecnologia da Informação e/ou pelo seu superior imediato.

A solicitação deve seguir o processo formal de solicitação e autorização, utilizando a ferramenta disponibilizada para este fim. É expressamente proibida a criação de quaisquer usuários privilegiados sem a correspondente solicitação e aprovação.

Para os ambientes SAP os acessos de usuários privilegiados possuem rastreabilidade das atividades realizadas e são monitorados pontualmente pela Diretoria de Tecnologia da Informação.

6.4. Revisões de acessos

Para garantir a eficácia dos controles implementados e manter a segurança sobre os acessos existentes a Diretoria de Tecnologia da Informação deverá comunicar os Owners a necessidade da revisão aos sistemas SAP, SAP (CRM), Mastersaf, Espaider, ZFA, EnergyIP, UtilityIQ, Ariba, Boletagem, Maxcom, Maxplan, CWSi, WBC Paradigma, Logos, LogosWeb, Sage, GTS, Diretório do Servidor de Arquivo, GISD (EO/DM), transações Críticas do SAP, o SAP_ALL e Função SE37 SAP ECC, conforme procedimento de controle de acesso definido para cada sistema. Cada responsável deve retornar com as ações de ajustes e remoções necessárias de acordo com a revisão para as devidas providências, caso não haja ações e ajustes informados os acessos serão mantidos até o próximo período de análise. Periodicidade de revisão de cada sistema se encontra no item 6.4.1.

São solicitados a relação de usuários e perfis das aplicações via CRM aos administradores responsáveis da aplicação (neste processo deve ser evidenciados a integridade da extração) e encaminhada aos Owners para revisão. Em casos de exceções a extração pode ser realizada via e-mail.

Os Owners definidos para revisão dos acessos devem ter cargos de no mínimo Coordenador/Supervisor, podendo possuir um delegado oficial, desde que ele tenha vínculo empregatício com o **Grupo CPFL**.

Para as revisões de acessos dos perfis descritos nas Matrizes de Segregação de Funções (SoD) dos sistemas Non-SAP, a Diretoria de Tecnologia da Informação deverá comunicar os respectivos Owners sobre a necessidade da revisão dos perfis de cada sistema. Cada responsável deve retornar com as ações de ajustes/validações para as devidas providências, caso não haja ações e ajustes informados os acessos serão mantidos até o próximo período de análise.
O Role Owner/responsável pela revisão deve manter registros das revisões realizadas para fins de auditoria e garantir a realização do controle, além de que caso exista divergências no acesso deverá abrir um chamado no Portal de Serviços para regularização.

6.4.1. Periodicidade de Revisão

Revisão deve ser realizada de acordo com a tabela abaixo:

Trimestralmente:

Transações Críticas do SAP

- SAP_ALL;
- Função SE37 SAP ECC

Semestralmente (preferencialmente em maio e novembro) dos sistemas informados abaixo**:**

Sistemas

- Ariba;
- Boletagem;
- CWSi-LEC;
- Diretórios de Rede/ Diretórios de Rede RGE;
- EnergyIP;
- Espaider;
- Mastersaf;
- Maxcom Comercialização/ Maxcom Geração;
- Maxplan;
- SAP;
- SAP (CRM);
- UtilityIQ;
- WBC-Paradigma;
- ZFA;
- Logos/LogosWeb;
- Sage;
- Gts.

Anualmente

- GISD (EO/DM);
- Matrizes de Segregação de Funções (SoD) dos sistemas Non-SAP

A Diretoria de Tecnologia da Informação deverá acompanhar a execução das revisões e caso não sejam feitas no período máximo de 30 dias após a comunicação, primeiramente será reportado o ocorrido ao respectivo superior do responsável pela revisão do acesso da área envolvida. Passados 15 dias de após o reporte ao superior imediato, o Diretor da área responsável será notificado e caberá à Diretoria de Tecnologia da Informação, bloquear o acesso do respectivo responsável ao ambiente de rede.

Fica estabelecido período mínimo de até 02 (dois) anos para a revisão geral dos fluxos de solicitação, aprovação e concessão de acessos deste documento, a fim de garantir que o processo de provisionamento dos acessos esteja aderente as políticas e práticas vigentes estabelecidas.

A conclusão das revisões deverá ser finalizada até o final do mês subsequente do seu início.

6.5. Registro das atividades das contas privilegiadas nos bancos de dados

Para garantir a eficácia dos controles implementados e manter a segurança sobre as informações, os sistemas SAP ECC, CRM, BIP, CCS, ECC, ECP, GRC, POP, BP1, ZFA, EnergyIP, Maxcom, Maxplan, CWSi, Boletagem, GISD (EO/DM), CRM Dynamics e Espaider possuem trilhas de auditoria habilitadas sobre as atividades realizadas pelas contas privilegiadas nos bancos de dados e revisadas anualmente pela Diretoria de Tecnologia da Informação.

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Ocorrência	Sistema CRM Dynamics	Backup	Por número de solicitação	Backup	Deletar
Chamado	GRC	Backup	Por número de solicitação	Backup	Deletar

8. ANEXOS

Não aplicável.

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Piratininga	EIQS	Heliane Pontes
Paulista	EIQS	Rafael Fedozzi
Paulista	EIS	Mateus Rocha

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
1.8	27/07/2012	Atualização do documento; Adequação à Norma “Governança de Documentos Gerenciais”
1.14	12/08/2015	Atualização do documento; Atualização dos sistemas
1.15	26/10/2016	Atualização do documento; Atualização dos sistemas
1.16	16/02/2018	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.17	01/12/2021	Revisão geral do documento e adequação a novas regras
1.18	03/03/2022	Atualização documento de referência
1.19	10/03/2022	Revisão geral do documento e adequação a novas regras
1.20	15/03/2022	Atualização do item 6.4 – Revisão dos acessos
1.21	12/04/2022	Atualização do item 6.4 – Revisão dos acessos
1.22	29/04/2022	Inclusão da Definição “Grupo CPFL”
1.23	20/06/2022	Atualização do item 6.4 – Revisão dos acessos.
1.24	20/09/2022	Atualização do item 6.4 – Revisão dos acessos
1.25	15/12/2022	Atualização do item 6.4 – Revisão dos acessos
1.26	13/03/2023	Atualização do item 6.4 – Revisão dos acessos
1.27	01/06/2023	Inclusão de novos sistemas (Sage, GTS, Logos, Logos Web e criação do item 6.4.1
1.28	05/06/2023	Inclusão do sistema SAP - CRM