 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES	2
4.	DOCUMENTOS DE REFERÊNCIA	2
5.	RESPONSABILIDADES	2
6.	REGRAS BÁSICAS	3
7.	CONTROLE DE REGISTROS.....	12
8.	ANEXOS	12
9.	REGISTRO DE ALTERAÇÕES	14

1. OBJETIVO

Descrever as etapas do processo de gerenciamento de acesso lógico aos usuários dos sistemas produtivos SAP.

2. ÂMBITO DE APLICAÇÃO


2.1. Empresa

Todas as empresas do **Grupo CPFL**.

2.2. Área

Todas as áreas da CPFL Energia que utilizam os sistemas SAP.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	1 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

3. DEFINIÇÕES

GESTOR DA INFORMAÇÃO: Nome atribuído à pessoa que é responsável por avaliar e aprovar as solicitações de acessos que são coerentes com as funções/ atividades dos usuários dos sistemas.

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;

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;

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;

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

4. DOCUMENTOS DE REFERÊNCIA

4.1. Internos

- Diretrizes de Segurança da Informação - GED 14369;
- Código de Conduta Ética - GED 19232;
- Norma para Gestão de Acessos - GED 14141;
- Procedimento de revisão das Matrizes de Segregação de Funções - GED 15261.

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. Usuário Solicitante


Preencher adequadamente os formulários na ferramenta GRC solicitando o acesso aos sistemas SAP necessário para a execução de suas atividades/funções diárias.

5.2. 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 aprovar ou reprovar formalmente através da ferramenta GRC.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	2 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Cabe também ao Superior solicitar a exclusão dos acessos do sistema SAP 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.

Aplicar sanções disciplinares aos colaboradores que não cumprirem a regra desta norma.

5.3. A cargo do Gestor da Informação

O Gestor da Informação é responsável pelos perfis de acessos do sistema SAP atribuído a todos usuários que utilizam o sistema. É de responsabilidade do Gestor da Informação avaliar se os perfis de acessos solicitados fazem sentido com as funções desempenhadas pelo usuário e se não há conflitos de segregação de função.

5.4. A cargo da Diretoria de Tecnologia da Informação

Analisar e executar a solicitação aprovada, informar o status das solicitações e comunicar o superior imediato quando identificar irregularidades de usuário.

6. REGRAS BÁSICAS

Os sistemas produtivos SAP são considerados críticos, em virtude da integração dos dados e processos das empresas listadas acima e possui um ambiente exclusivo e dedicado.

O gerenciamento de usuários e perfis de acesso é um conjunto de procedimentos aplicados ao ambiente de tecnologia da empresa para controlar a concessão, exclusão, *reset*/bloqueio/desbloqueio, alteração e criação de perfis dos acessos de seus colaboradores aos ambientes produtivos SAP.

Existem 4 processos distribuídos em 9 tipos de solicitações:


1. Liberação, Alteração e Renovação de acesso:
 - Criar Usuário
 - Modificar Conta Usuário
 - Dados Mestres de Usuário
2. Exclusão de Acesso.
3. Criação, Alteração e Exclusão de Perfil de acesso.
4. *Reset*, Esqueci minha senha, Bloqueio e Desbloqueio de acesso.

6.1 Liberação, Alteração e Renovação de Acesso.

6.1.1. Criar Usuário / Modificar Conta Usuário

Usuário Solicitante

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	3 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Para solicitar a liberação ou alteração de acesso aos ambientes produtivos SAP é necessário que o usuário possua acesso à rede corporativa ou, o solicite, preenchendo o formulário disponível na intranet do grupo CPFL, no Portal de Serviços.

Com acesso à rede corporativa o usuário deve solicitar acesso aos ambientes produtivos SAP, acessando a ferramenta GRC – Gestão de Acesso, no seguinte endereço <https://mapp.cpfl.com.br>, e deve informar o ambiente e as funções necessárias para executar as atividades de seu dia a dia.

Estas funções podem ser solicitadas por processo/sub processo, grupos, transações ou modelado por usuário existente.

Os seguintes campos são de preenchimento obrigatório no momento da criação do chamado no GRC:

- Área funcional;
- Motivo da Solicitação;
- ID do usuário;
- Primeiro Nome;
- Sobrenome;
- E-mail;
- Gerente;
- Empresa;
- Sistemas;
- Funções;
- Número do Contrato – Terceiro (*);
- Data Término Contrato – Terceiro (*).

(*) Quando o colaborador não tiver vínculo empregatício com as empresas do grupo CPFL Energia deve ser informado, no entanto, o campo “Data Término Contrato – Terceiro” é automaticamente preenchido com os dados do contrato informado no campo “Número do Contrato – Terceiro”.

Quando o usuário concluir a criação da solicitação, uma notificação é enviada ao Superior Imediato para aprovação do acesso.

Quando um novo colaborador efetivo, com vínculo empregatício com as empresas do grupo CPFL Energia, é registrado no Sistema SAP HR, automaticamente é criada uma solicitação de “Criação de usuário no portal ESS” no GRC com perfil básico no ECC e Portais. Para esta solicitação não há necessidade de aprovação do superior imediato.

Obs: Solicitações paradas a mais de 45 dias na mesma etapa, seja com o Role Owner ou Gestor Imediato poderão ser rejeitadas automaticamente.


6.1.2. Superior Imediato

Após o recebimento da solicitação de inclusão de acesso, o superior imediato deve analisar a solicitação do usuário frente suas atividades/funções, podendo aprová-la ou reprová-la.

6.1.3. Responsável da Função

Ao receber a solicitação aprovada pelo superior imediato do solicitante, o responsável pela função, denominado como *Role Owner* na ferramenta GRC, deve analisar o pedido e identificar possíveis conflitos

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	4 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

entre a solicitação e as funções desempenhadas pelo usuário solicitante. Após a análise deve reprovar ou aprovar a solicitação.

Uma vez aprovada pelo Superior Imediato e Responsável da Função (*Role Owner*), a solicitação é executada e encerrada, desde que não existam conflito de segregação de funções.

6.1.4. Roles Básicas

6.1.4.1 Colaboradores

Assim que contratados o colaborador tem os acessos abaixo pré-aprovados, não sendo necessários a coleta de aprovações:

Ambientes	Funções	Descrição
ERPCLNT350	ZECC_GRH0000_GRH_MS	Dados básicos de HR Colaborador CLT
ERPCLNT350	ZECC_AUTOGER	Função básica para todos os colaboradores CPFL
GP1CLNT350	ZGRC_CAC0101_CAC_MS	Acesso básico GRC (Solic. Acesso/Esqueci Minha Senha)
GR1CLNT350	ZGR1_AUTOGER_ESS_MS	Acesso ao Portal Corp (Guia Gestão de Acessos e Guia CPFL Colaborador)
SFPCLNT350	ZFIO_USER_BASIC0_FIORI	Acesso Básico no Fiori (Programação de Férias)
CXHCLNT100	ZHXM_GRH0000_GRH_MS	Dados básicos de HR Colaborador CLT


6.1.4.2 Gestor/Gerente

Caso possua o cargo de gestor/gerente tem os acessos abaixo pré-aprovados, não sendo necessários a coleta de aprovações:

Ambientes	Funções	Descrição
ERPCLNT350	ZECC_GRH0001_GRH_MS	Dados básicos de HR Colaborador CLT
GP1CLNT350	ZGRC_CAC0102_CAC_MS	Acesso básico GRC (Solic. Acesso/Esqueci Minha Senha)
GR1CLNT350	ZGR1_AUTOGER_GES_MS	Acesso ao Portal Corp (Guia Gestão de Acessos e Guia CPFL Colaborador)
SFPCLNT350	ZFIO_APR0001_FIO_CP	Acesso Básico no Fiori (Programação de Férias)

6.1.4.3 Coordenadores/Líderes

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	5 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Caso possua o cargo de coordenador/líder tem os acessos abaixo pré-aprovados, não sendo necessários a coleta de aprovações:

Ambientes	Funções	Descrição
ERPCLNT350	ZECC_GRH0003_GRH_MS	Dados básicos de HR Colaborador CLT
GP1CLNT350	ZGRC_CAC0102_CAC_MS	Acesso básico GRC (Solic. Acesso/Esqueci Minha Senha)
GR1CLNT350	ZGR1_AUTOGER_LID_MS	Acesso ao Portal Corp (Guia Gestão de Acessos e Guia CPFL Colaborador)
SFPCCLNT350	ZFIO_APR0001_FIO_CP	Acesso Básico no Fiori (Programação de Férias)

6.1.4.4 Role Owner

Caso seja Role Owner tem os acessos abaixo pré-aprovados, não sendo necessários a coleta de aprovações:

Ambientes	Funções	Descrição
GP1CLNT350	ZGRC_CAC0103_CAC_MS	AC - Aprovação de solicitações - Role Owner
SFPCCLNT350	ZFIO_GRCAC_GRUPO_004	Acesso Básico no Fiori (Programação de Férias)

Tecnologia da Informação

Caso a solicitação do usuário gerar situação de conflito de segregação de função e não seja possível remediar ou não tenha um controle compensatório já definido, a área de Tecnologia da Informação informará a área de negócio responsável pelo processo que em conjunto com o *Role Owner*, devem definir a ação mitigatória (controle compensatório) para o risco, informando a Gerência de Compliance, para avaliação.


Os controles compensatórios estão definidos para todos os riscos e são revisados conforme Procedimento de revisão das Matrizes de Segregação de Funções (GED 15261).

Dados Mestres de Usuário (Renovação de Acesso)

Solicitante

Quando da expiração da data de validade de acesso em qualquer ambiente SAP dos colaboradores que não tiverem vínculo empregatício com as empresas do grupo CPFL Energia, outro usuário deverá solicitar

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	6 de 14


 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

a renovação do acesso deste usuário com a data de expiração vencida, através do “GRC – Gestão de Acesso”, tipo de solicitação Dados Mestre de Usuário, informando o número do contrato e a data de término e gestor do contrato.

Quando o usuário concluir a criação do chamado, uma notificação é enviada ao e-mail do superior imediato indicado na solicitação para aprovação.

Cópia Não Controlada

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	7 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Superior Imediato

Após o recebimento da solicitação de Dados Mestres de Usuário, o superior imediato deve analisar a solicitação, podendo aprová-la ou reprová-la.

Tecnologia da Informação

Após a aprovação, o chamado é enviado automaticamente para a área de Tecnologia da Informação efetivar a alteração.

6.2 Exclusão de Acesso

A solicitação de exclusão de acesso aos ambientes produtivos SAP é realizada da seguinte forma:

- Quando o desligamento de estagiário ou colaborador com vínculo empregatício com as empresas do Grupo CPFL Energia o Departamento de Recursos Humanos é responsável em enviar e-mail informando o desligamento para a exclusão dos acessos, após o recebimento do e-mail a área de Tecnologia da Informação deve efetuar a exclusão dos acessos.
- Quando do encerramento da atividade/função do colaborador, sem vínculo empregatício, ou quando do término do contrato de Prestação de Serviços, sob sua responsabilidade, o Gestor do contrato deve solicitar, via ferramenta GRC, a eliminação do acesso.

6.3 Criação, Alteração e Exclusão de Perfil de acesso

Deverá ser solicitado, via GRC, tipo de solicitação “Falta de Acesso (Ajuste de Objeto)”, quando o usuário já possui a transação em seu perfil de acesso e ao executá-la ocorre um erro por falta de acesso em um determinado objeto de autorização dessa transação.

O usuário deverá anexar a tela de erro (extraída pela transação “/NSU53”) logo após a mensagem do erro, para identificar o objeto de autorização que está com a falta de acesso e anexá-lo à solicitação.

A criação, alteração e exclusão de Perfil de Acesso nos sistemas SAP, somente podem ser solicitadas pelo Responsável da função (*Role Owner*).

Responsabilidade sobre a definição de “Role Owner” pertence ao Superior/Gerente imediato.

Responsável da Função

Para solicitar a criação ou alteração de perfil de acesso, deve acessar a ferramenta GRC no seguinte endereço <https://mapp.cpfl.com.br>, tipo de solicitação “Falta de Acesso (Ajuste de Objeto)” e deve informar os perfis a serem criados, alterados e a justificativa.


Tecnologia da Informação

Ao receber a solicitação de criação ou alteração de perfil de acesso, a área de Tecnologia da Informação deve verificar se constam as informações necessárias para prosseguir o processo.

Caso o chamado não esteja devidamente preenchido, deverá reprová-lo.

Caso as informações sejam suficientes deve realizar uma análise de risco de função.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	8 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Não serão criados novos perfis ou alterados perfis existentes caso existam riscos.

6.4 Reset, Esqueci minha senha, Bloqueio e Desbloqueio de acesso.

6.4.1 Reset

Quando o usuário não se lembrar da senha, este deve abrir um chamado na ferramenta GRC.

Caso o solicitante seja diferente do usuário a nova senha será encaminhada ao e-mail do usuário. Caso o solicitante e usuário sejam a mesma pessoa, a nova senha será informada na própria solicitação. Essa senha deverá ser alterada no primeiro *login*.

6.4.2 Esqueci minha senha

A ferramenta GRC disponibiliza também a opção de “Esqueci minha senha”, onde o usuário deve cadastrar inicialmente o número do CPF e RG, e para realizar o *reset*, é necessário apenas informar os dados e a nova senha é encaminhada ao e-mail do solicitante.

6.4.3 Desbloqueio

Quando o usuário não se lembrar da senha, e por qualquer motivo seu acesso aos sistemas SAP foi bloqueado, este deve abrir um chamado na ferramenta GRC, solicitando o desbloqueio do acesso.

O desbloqueio também será feito de forma automática a cada 30 minutos para os usuários bloqueados por demasiadas tentativas de *login* incorreto, dispensando a criação de uma solicitação no GRC.

6.4.4 Bloqueio

O usuário poderá solicitar o bloqueio de seu acesso aos sistemas SAP quando for se ausentar da empresa por um período longo, este deve abrir um chamado na ferramenta GRC e solicitar o bloqueio.

6.5 Encerramento das Solicitações

Superior imediato/ Responsável da Função (*Role Owner*) / Tecnologia da Informação

Caso o superior imediato, o Responsável da Função (*Role Owner*) ou a área de Tecnologia da Informação rejeitar a solicitação, este deve registrar o motivo no momento da rejeição e o solicitante recebe um e-mail informando a rejeição da solicitação.

Tecnologia da Informação

Após a confirmação do atendimento, deve descrever o atendimento e a solicitação é automaticamente concluída e o solicitante recebe um e-mail informando a conclusão da solicitação.


6.6 Acompanhamento do Status das Solicitações

Usuário Solicitante

O usuário solicitante deve consultar a ferramenta GRC sempre que necessário para verificar o andamento de sua solicitação, em “Minhas Solicitações”, principalmente na seção “Status da Instância”.

6.7 Revogação de acesso por não utilização

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	9 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

CXH

Quinzenalmente, os usuários que não acessam o sistema CXH há mais de 42 dias, com exceção dos Gerentes, Diretores, VPs, Presidente, terão os perfis de acesso removidos, permanecendo apenas as funções mínimas de acesso para o SAP RH.

As contas não podem ser bloqueadas ou eliminadas em virtude do acesso ao SAP RH.

ERP

Quinzenalmente, os usuários que não acessam o sistema ERP há mais de 42 dias, com exceção dos Gerentes, Diretores, VPs, Presidente, terão os perfis de acesso removidos, permanecendo apenas as funções mínimas de acesso para o SAP RH e função básica de autorizações gerais.

As contas não podem ser bloqueadas ou eliminadas em virtude do acesso ao SAP RH.

CRP/CCP

Quinzenalmente, os usuários que não acessam o sistema CRP e CCP há mais de 42 dias, com exceção dos Gerentes, Diretores, VPs e Presidente terão os acessos removidos.

Os usuários que acessam o CRP, no entanto não acessam o CCP, devem permanecer com acesso ao CRP, devido à atribuição dos usuários na estrutura e vice e versa.

Demais ambientes produtivos SAP, quinzenalmente, os usuários que não acessam o sistema há mais de 42 dias, com exceção dos Gerentes, Diretores, VPs e Presidente, terão os acessos bloqueados.

Não se aplicam nesta regra as contas classificadas como comunicação, sistemas e serviços nos ambientes, por serem utilizadas pelas aplicações.

6.8 Revisão periódica

Semestralmente, a Diretoria de Tecnologia da Informação deverá comunicar aos responsáveis das funções, denominados *Role Owner*, da responsabilidade pela revisão dos acessos às funções sob a sua responsabilidade nos sistemas BIP, ECP, GP1, BP1, PNP, SFP, GR1, FMP, ERP, CCP e CRP através da ferramenta GRC.


A ferramenta GRC manterá o log das revisões realizadas, registrando as respectivas ações de autorização ou remoção, conforme a necessidade.

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. Passando 15 dias 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 *Role Owner* ao ambiente de rede.

6.9 Substituição do Role Owner

- Em caso de substituição de Role Owner existente no processo por motivo de ausência temporária (licença, férias) ou mudança de área e/ou cargo; este deve solicitar através da ferramenta GRC (Gestão de Acesso) na opção de "Dados Mestres de Usuário" a sua substituição, informando o novo colaborador que assumirá as atividades.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	10 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

A solicitação requer aprovação do superior/gestor imediato do novo *Role Owner* indicado e o preenchimento e envio do “Termo de Responsabilidade – Role Owner” anexo a requisição.

O compartilhamento de credenciais de acesso de colaboradores não é permitido no Grupo CPFL e em caso de descumprimento o colaborador fica sujeito as medidas disciplinares conforme GED 19232 - Código de Conduta Ética.

- Em caso de desligamento de Role Owner vigente, o superior imediato assume automaticamente as responsabilidades pelas aprovações e atribuições até que seja nomeado um novo substituto. O Time de Segurança de TI é responsável pela notificação e formalização através de e-mail ao gestor que assumirá a responsabilidade e ao respectivo Diretor. Nesta ocasião é enviado o “Termo de Responsabilidade – Role Owner” ao gestor para as devidas aprovações e este e-mail e termo são as evidências de formalização deste processo. O time de Segurança de TI registra a solicitação no GRC e inclui este e-mail de formalização no chamado para o provisionamento do perfil de Role Owner de acordo com o item 6.1.4.4 deste documento.

6.10 Delegação de aprovação

O Superior Imediato e o *Role Owner* podem delegar a sua caixa de aprovação do GRC para outro usuário por um tempo determinado.

Esta delegação se aplica apenas à aprovação das solicitações do GRC, para a atividade de reafirmação de função deve seguir o item acima de Substituição do *Role Owner*.

Nunca deve emprestar as credenciais de acesso do colaborador que se ausentará, caso isso ocorra esta atitude poderá ser aplicada medidas de sanções como descrito na norma nº 19232 - Código de Conduta Ética.

Em caso de mudança de área, o acesso deverá ser revogado e solicitado os novos acessos necessários para exercer suas atividades.

É dever do colaborador informar a liderança e abrir um chamado para remover os acessos, não devendo ficar com o acesso não permitido.

6.11 Parâmetros de configuração de acesso dos Sistemas SAP

Todos os usuários cadastrados no sistema possuem parâmetros de acesso ao sistema. São eles:


- Tamanho da senha: 8 caracteres;
- Tempo de expiração da senha: 30 dias;
- Bloqueio de usuário por tentativas inválidas: 3;
- Restrição de últimas senhas utilizadas: 5;
- Tabela de exceção de senhas: USR40.

6.12 Mudança de área

Em caso de mudança de área, o acesso deverá ser revogado e solicitado os novos acessos necessários para exercer suas atividades.

É dever do colaborador informar seu superior imediato e abrir um chamado para remover os acessos, não devendo ficar com os acessos não permitidos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	11 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

7. CONTROLE DE REGISTROS

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

8. ANEXOS

Termo de Responsabilidade – Role Owner.

 USO INTERNO	TERMO DE RESPONSABILIDADE <i>Role Owner</i>
--	---

Este termo tem por finalidade de confirmar a realização dos e-learnings e a leitura das normas indicadas sobre as atividades do Role Owner no Portal FIORI (<https://mapp.cpfl.com.br/>)

Atividades:

- Aprovar ou rejeitar os acessos solicitados pelos colaboradores.
[http://portais.cpfl.com.br/sites/gestao-do-conhecimento/ti/Paginas/GRC-Como-aprovar-solicitacao-Modificar-Conta-\(Estagio-Role-Owner\).aspx](http://portais.cpfl.com.br/sites/gestao-do-conhecimento/ti/Paginas/GRC-Como-aprovar-solicitacao-Modificar-Conta-(Estagio-Role-Owner).aspx)
- Revisar semestralmente os acessos dos colaboradores
<http://portais.cpfl.com.br/sites/gestao-do-conhecimento/ti/Paginas/GRC-Como-aprovar-solicitacao-de-revisao-de-Acesso-de-Usuario%28UAR%29.aspx>
- Revisar anualmente as Matrizes de Segregação de Funções

Normas:

- GED 14669 - Procedimento de Controle de acesso aos Sistemas SAP
- GED 15261 - Procedimento de revisão das Matrizes de Segregação de Funções

E-learnings (disponíveis no Dicas de TI): <http://portais.cpfl.com.br/sites/gestao-do-conhecimento/ti/Paginas/SAP-GRC12.aspx>


- Aprovar solicitações - Avançada
- Delegar aprovação
- Reafirmação de Funções (Revisão de Acessos dos Usuários)
 Como aprovar os acessos dos usuários
 Como remover os acessos dos usuários

Nome do usuário:	
Matrícula:	Diretoria:
Departamento:	
Cargo/Função:	
Superior Imediato:	
Empresa:	

Declaro estar ciente das minhas atividades de Role Owner e que realizei os e-learnings no Portal GRC e a leitura dos GEDs indicados acima e, comprometo-me a seguir todas as orientações neles estabelecidos.


_____ Usuário (Assinatura)	_____ Gestor (Assinatura)
----------------------------------	---------------------------------

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	12 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

Cópia Não Controlada

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	13 de 14

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de acesso aos Sistemas SAP

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIGV	Rafael Fedozzi
Paulista	EIS	Mateus Rocha
RGE	EIS	Everton Duarte

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
1.14	14/06/2018	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.15	30/05/2019	Revisão dos itens 6.10, 6.11 e inclusão do item 6.12.
1.16	15/09/2020	Revisão geral do documento
1.17	03/03/2022	Funções básicas
1.18	08/03/2022	Termo de Responsabilidade de Role Owner
1.19	01/04/2022	Funções básicas
1.20	13/04/2022	Revisão geral do documento
1.21	13/07/2022	Substituição de Role Owner
1.22	19/10/2022	Solicitações paradas a mais de 45 dias na mesma etapa
1.23	12/01/2023	Inclusão de funções básicas e inclusão do ambiente CXH

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14669	Tático	25.0	Emerson Cardoso	23/10/2023	14 de 14