 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

Sumário

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

1. OBJETIVO

Esta norma tem como objetivo de descrever as etapas do processo de gerenciamento de acesso lógico de usuários à rede corporativa.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas com participação direta da CPFL Energia.

2.2. Área

Todas as áreas da CPFL Energia.

3. DEFINIÇÕES


Os principais termos contidos nesta norma envolvem as seguintes definições:

CRM DYNAMICS: Ferramenta utilizada para registro das Ocorrências;

PORTAL DE SERVIÇOS: Ferramenta para registro de Ocorrências no CRM Dynamics. Acesso através da intranet da CPFL;

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

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	1 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

INTUNE: Serviço de gerenciamento de mobilidade empresarial, proporciona recursos abrangentes para gerenciar dispositivos móveis.

4. DOCUMENTOS DE REFERÊNCIA

Internos

- GED 14369 – Diretrizes de Segurança da Informação;
- Código de Ética e de Conduta Empresarial do grupo CPFL;
- GED 14141 – Norma para gestão de Acessos;
- GED 16009 - Manual de Reset e Desbloqueio Automático de Senha da Rede;
- GED 17037 – Jornada de Trabalho.

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 no Portal de Serviços solicitando o acesso à rede corporativa necessário para a execução de suas atividades/funções diárias.

5.2. Superior Imediato

Tem como responsabilidade avaliar as solicitações e aprovar ou reprovar formalmente através do Portal de Serviços.

Cabe também ao Superior solicitar a exclusão dos 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.


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

5.3. 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

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	2 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

O gerenciamento de usuários é um conjunto de procedimentos aplicados ao ambiente corporativo de tecnologia da informação da empresa para controlar a concessão, exclusão, reset/bloqueio/desbloqueio e alteração dos acessos de seus colaboradores e terceiros à rede corporativa.

O processo está dividido em três etapas:

- Criação de Acesso;
- Renovação de Acesso;
- Exclusão de Acesso;
- Reset / Bloqueio e Desbloqueio de Acesso.

6.1. Solicitação de Criação de Acesso

Usuário Solicitante

Para solicitar a criação de acesso à rede corporativa, o usuário solicitante deve preencher o formulário via Portal de Serviços, disponível na intranet do grupo CPFL e deve informar os seguintes dados, como o nome completo, matrícula, e-mail, telefone, cidade, departamento, centro de custo, empresa, área, função e, número do contrato de prestação de serviço e sua data de término quando o colaborador não tiver vínculo empregatício com as empresas do grupo CPFL Energia.

Deve descrever os acessos desejados e a justificativa para criação do acesso, em seguida a solicitação é encaminhada ao Superior imediato para aprovação.

Com esta solicitação, os acessos básicos como: acesso à rede corporativa, internet, Portal Multi, e-mail e Lync serão concedidos.

Quando um novo colaborador efetivo, com vínculo empregatício com as empresas do grupo CPFL Energia é registrado no Sistema SAP HR, automaticamente será criado o acesso básico como: acesso à rede corporativa, internet, Portal Multi, e-mail e Lync. Para esta solicitação não há necessidade de aprovação do superior imediato.

Estão excluídos deste processo automático Diretores, VPs e Presidente.

Para os usuários que não forem criados automaticamente devem seguir o procedimento de solicitação pelo Portal de Serviços.

Superior imediato


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

Tecnologia da Informação

Após receber a solicitação aprovada, a área de Tecnologia da Informação deve executar a criação do acesso solicitado, ou caso a solicitação estiver preenchida incorretamente, deve rejeitar a solicitação.

6.2. Solicitação de Renovação de Acesso

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	3 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

Caso o acesso do colaborador esteja expirado, outro usuário deverá solicitar a renovação de acesso à rede corporativa, no qual deve preencher o formulário via Portal de Serviços, disponível na intranet do grupo CPFL e deve informar os seguintes dados, como o nome completo, matrícula, e-mail, telefone, cidade, departamento, centro de custo, empresa, área, função e, número do contrato de prestação de serviço e sua data de término quando o colaborador não tiver vínculo empregatício com as empresas do grupo CPFL Energia.

Deve descrever os acessos desejados e a justificativa para renovação do acesso, em seguida a solicitação é encaminhada ao Superior imediato para aprovação.

Com esta solicitação, os acessos básicos como: acesso à rede corporativa, internet, Portal Multi, e-mail e Lync serão renovados.

Superior imediato

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

Tecnologia da Informação

Após receber a solicitação aprovada, a área de Tecnologia da Informação deve executar a renovação do acesso solicitado, ou caso a solicitação estiver preenchida incorretamente, deve rejeitar a solicitação.

6.3. Solicitação de Exclusão de Acesso.

A solicitação de exclusão de acesso à rede corporativa deve ser formalizada e comunicada por:

Recursos Humanos

Quando do desligamento de estagiário ou colaborador com vínculo empregatício com as empresas, o departamento de Recursos Humanos é responsável por enviar e-mail informando o desligamento para a exclusão dos acessos.

Gestor

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 deve solicitar via Portal de Serviços a revogação do acesso.


6.4. Revogação de acesso por não utilização.

Os usuários que não utilizarem a rede há mais de 6 semanas e não alterarem a senha de acesso passados 15 (quinze) dias da data expiração das senhas, terão suas contas automaticamente bloqueadas, através do script de bloqueio executado diariamente.

As contas de usuário criadas para atender as necessidades técnicas do ambiente operacional e, as que servem apenas de interface entre sistemas não se enquadram nesta regra.

Usuários que detêm permissão de escrita para dispositivos USB e que não registram atividades nos últimos 180 dias terão seu acesso restrito exclusivamente à leitura. Adicionalmente, aqueles que não fazem uso de dispositivos USB ao longo de 120 dias terão seus privilégios removidos.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	4 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

Usuários inativos por mais de 6 semanas serão excluídos da política de acesso condicional para o Intune.

6.5. Solicitação de Reset, Bloqueio e Desbloqueio de acesso.

Usuário Solicitante

Reset

Quando o usuário não se lembrar da senha da rede (AD), outro usuário deverá solicitar o reset através do Portal de Serviços, disponível na intranet do grupo CPFL, em seguida a solicitação é encaminhada ao Superior imediato do usuário que esqueceu a senha para aprovação.

Após receber a solicitação aprovada, a área de Tecnologia da Informação deverá executar o Reset na rede corporativa, gerar uma nova senha aleatória e enviar ao superior imediato com cópia ao próprio usuário que teve a senha resetada.

É disponibilizada também a opção de auto reset, onde o usuário deve cadastrar inicialmente o número de seu celular, através do link <http://resetdesenha>. Para colaboradores da CPFL Atende, com cargo Atendente de Telemarketing, o cadastro deverá ser realizado com o número do CPF e RG.

Para realizar o reset da senha, é necessário acessar a opção “Reset de Senha/Desbloqueio” na tela de login da rede e informar os dados cadastrados.

Bloqueio

A conta do usuário poderá ser bloqueada mediante solicitação através do Portal de Serviços, disponível na intranet do grupo CPFL, encaminhando-o ao seu superior imediato para aprovação.

Superior imediato

Após o recebimento da notificação de solicitação de Bloqueio, deverá verificar se o pedido é justificado e aprová-lo ou reprová-lo.

Tecnologia da Informação


Após receber a solicitação, a área de Tecnologia da Informação deve executar o bloqueio do acesso solicitado, ou caso a solicitação estiver preenchida incorretamente, deve rejeitar a solicitação.

Desbloqueio

Quando o acesso do usuário estiver bloqueado, esse deverá solicitar o desbloqueio para a Central de Atendimento, através do ramal 8002 (Sede) ou 922-8002 para demais localidades ou através do Portal de Serviços.

O desbloqueio é feito de forma automática a cada 15 minutos para os usuários bloqueados por demasiadas tentativas de login incorreto, dispensando a criação de uma solicitação no portal de serviços.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	5 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

É disponibilizada também a opção de auto desbloqueio, onde o usuário deve cadastrar inicialmente o número de seu celular, através do link <http://resetdesenha>. Para colaboradores da CPFL Atende, com cargo Atendente de Telemarketing, o cadastro deverá ser realizado com o número do CPF e RG. Para realizar o desbloqueio da senha, é necessário acessar a opção “Reset de Senha/Desbloqueio” na tela de login da rede e informar os dados cadastrados do CPF e RG.

6.6. Encerramento das Solicitações.

Superior imediato

Caso a solicitação seja rejeitada, registra o motivo da rejeição e informa o usuário solicitante.

Tecnologia da Informação

Com a conclusão da solicitação informa o usuário solicitante.

Caso a solicitação seja rejeitada, registra o motivo da rejeição e informa o usuário solicitante.

6.7. Acesso Remoto

Todo acesso remoto aos sistemas da CPFL é realizado através de VPN (Virtual Private Network). Para o acesso é necessário que o MFA esteja ativado, e com client atualizado.

Para liberação de acesso à VPN o usuário deve preencher o formulário via Portal de Serviços, (todos os campos devem ser informados, mesmo que o campo não seja obrigatório) disponível na intranet do grupo CPFL e deve informar os tipos de acesso desejado.

Quando o usuário concluir a criação da solicitação, será enviada uma notificação ao e-mail do superior imediato para aprovação.

Após a aprovação do superior imediato e Diretor quando aplicável, a solicitação é encaminhada para a área de Segurança da Informação para aprovação, após isso a área de Tecnologia da Informação irá conceder o acesso solicitado. Nos casos em que o acesso é solicitado para um ambiente específico não contemplado pelas liberações da VPN padrão, este será encaminhado para a Gerência de Serv. Infra. e Operações de TI para validação técnica e criação de Grupo de VPN específico caso aprovado.

As configurações do software cliente de VPN devem obedecer aos critérios de segurança estabelecidos pelo Departamento de Tecnologia da Informação.

A autenticação de acesso da VPN segue os parâmetros de acesso descritos no item 4.


Revogação de acesso

A revogação do acesso à VPN será aplicada aos usuários que não efetuarem a autenticação por um período superior a 6 semanas.

Restrições

Não será concedido acesso a estações de trabalho através da VPN para conexão remota (RDP) ou mesmo para acesso a pastas compartilhadas da estação.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	6 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

6.8. Parâmetros de acesso dos usuários

Todos os usuários cadastrados à rede corporativa possuem parâmetros de acesso. São eles:

- Tamanho mínimo da senha: 8 caracteres;
- Tempo de expiração da senha: 60 dias;
- Bloqueio de usuário por tentativas inválidas: 10;
- Restrição de últimas senhas utilizadas: 4;
- Complexidade de senhas: habilitado;
- MFA ativado.

6.9. Contas genéricas da rede corporativa

Toda conta genérica da rede corporativa deverá ter um responsável associado, essa associação será documentada na ferramenta de administração de usuários para garantir a sua rastreabilidade.

6.10. Revisão periódica

A revisão dos acessos é realizada para os Diretórios de Rede e são de responsabilidade das respectivas áreas de negócio e na periodicidade definida conforme Norma para Gestão de Acessos aos Sistemas de TI (GED 14141).

7. CONTROLE DE REGISTROS

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

8. ANEXOS


Não aplicável.

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIG	Rafael Sartoreto Fedozzi
Paulista	EIS	Mateus Augusto Pereira Rocha
Paulista	EIS	Luciana Rodrigues Lopes

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	7 de 8

 Uso Interno	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Controle de Acessos a Rede Corporativa.pdf

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
1.11	31/10/2017	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.12	12/04/2019	Atualização do item: 6.8. Parâmetros de acesso dos usuários
1.13	23/12/2021	Revisão periódica
1.14	10/02/2023	Revisão periódica – MFA ativado
1.15	24/02/2023	Revisão geral do documento
1.16	05/06/2023	Atualização do item: 6.4.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
14665	Tático	18.0	Emerson Cardoso	26/12/2023	8 de 8