	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

Sumário

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

1. OBJETIVO

Este documento serve como medida para apoiar a segurança da informação, para que sejam implementadas regras para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

2. ÂMBITO DE APLICAÇÃO

Esta norma se aplica a todos os usuários (clientes, prestadores de serviços, estagiários, empregados) que utilizam o ambiente do **Grupo CPFL** para acesso a serviços computacionais.

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:

Segurança da Informação - proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no **Grupo CPFL**.

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.

N.Documento: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 1 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

Incidente em Segurança da Informação - qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do Grupo ou ameaçar a segurança da informação.

Usuário - qualquer pessoa (empregados, clientes, visitantes, estagiários, empregados temporários, prestadores de serviços, colaboradores) que possua ou não ligação com o **Grupo CPFL**, e que necessite de acesso a um sistema ou recurso computacional do **Grupo CPFL**.

VPN - a sigla VPN vem do inglês Virtual Private Network, que em tradução livre significa Rede Virtual Privada. Ela utiliza a internet para se conectar a uma determinada localidade e assim poder usar seus serviços.

4. DOCUMENTOS DE REFERÊNCIA

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de segurança Código de prática para a Gestão da Segurança da Informação.

Norma NBR ISOIEC 17799 - Tecnologia da Informação - Técnicas de Segurança - Código de Diretrizes de Segurança da Informação do **Grupo CPFL**.

5. RESPONSABILIDADES

Usuário


- Manter sigilo das informações de acesso ao ambiente de rede do **Grupo CPFL** e da conexão remota, sendo de sua total e exclusiva responsabilidade qualquer operação realizada por meio de suas credenciais de acesso;
- Comunicar imediatamente à área de Segurança da Informação, qualquer situação que coloque em risco o acesso ao ambiente da rede de dados do **Grupo CPFL**;
- Informar seu gestor quando forem identificados direitos de acesso remoto desnecessários à execução dessas atividades.

Gestor

- Solicitar e/ou revogar as credenciais de acesso remoto dos usuários sob sua gestão;
- Conscientizar os usuários em seu domínio administrativo quanto às orientações presentes neste documento e nas boas práticas de segurança;
- Comunicar imediatamente ao setor de Segurança da Informação, caso verifique qualquer ameaça, vulnerabilidade ou situação que possa colocar em risco o ambiente computacional em questão; e
- Manter atualizada relação de usuários e seus papéis para que, de forma contínua, seja verificada a política de acessos mínimos e com isso a adequação dos perfis de acesso dos respectivos usuários.

Segurança da Informação

N.Documento: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 2 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

- Administrar os acessos remotos ao ambiente de rede de dados do **Grupo CPFL**;
- Manter a disponibilidade, integridade e confidencialidade em todo o ambiente computacional que suporta a solução de acesso remoto "client-to-site";
- Monitorar todo o ambiente de modo a identificar proativamente anomalias e acessos maliciosos;
- Manter os registros de acesso para fins de auditoria respeitando a legislação e as boas práticas de mercado;
- Manter mecanismos de segregação de acesso lógico entre os ambientes de acesso remoto e os recursos computacionais em ambiente de rede local controlando o acesso por meio de políticas de acessos mínimos;
- Manter registro histórico de solicitações de criação e revogação de usuários para fins de auditoria e controle;

6. REGRAS BÁSICAS

6.1 Trabalho remoto

O **Grupo CPFL** permite a atividade de trabalho remoto e define as condições e restrições para o uso do trabalho remoto. Onde considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

A segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do local;

O ambiente físico proposto para o trabalho remoto;

Os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;

O fornecimento de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;


O ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;

O uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;

Políticas e procedimentos para prevenir disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular, acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), o qual pode ser restringido por lei;

Acordos de licenciamento de *software* que podem tornar as organizações responsáveis pelo licenciamento do *software* cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou partes externas;

N.Documento: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 3 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------

 <p>CPFL ENERGIA Uso Interno</p>	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

Requisitos de firewall e proteção antivírus.

6.2 Procedimentos de Acesso Remoto

O acesso à VPN, está restrito a jornada de trabalho em contrato e terceiros.

Para liberação de acesso aos usuários que não se enquadram nos cargos acima, serão considerados regime de exceção e deverão ter o acesso aprovado pelo respectivo Diretor.

Todo acesso remoto aos sistemas do **Grupo CPFL** é realizado através de VPN (Virtual Private Network).

Para liberação de acesso à VPN o usuário deve preencher o formulário via Portal de Serviços, 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 Tecnologia da Informação para 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.

6.3 Revogação de acesso

Todo mês de março o acesso será revogado dos usuários que tiveram a liberação em regime de exceção.

6.4 Revisão periódica


Mensalmente a área de TI enviará para a Diretoria de Gestão de Pessoas e Performance – PG, a relação de todos os usuários com acesso a VPN para que seja verificada a condição de Cargo de Confiança e os identificados como em Regime de Exceção serão informados aos Vice-Presidentes das Áreas e/ou CEO para acompanhamento por esta diretoria.

É responsabilidade de cada Diretoria solicitar a revogação do acesso via chamado quando houver necessidade.

6.5 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: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 4 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

6.6 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: 5;
Restrição de últimas senhas utilizadas: 4;
Complexidade de senhas: habilitado.

6.7 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.

6.8. Premissas

- As liberações de acesso à Terceiros (Prestadores / Fornecedores), devem conter no registro da Demanda: Documento NDA com Validade / Prazo do Contrato assinados e responsabilizados. Autorização do Líder no **Grupo CPFL** como também os acessos necessários via Firewall e sua justificativa para tal acesso.
- Os colaboradores têm permissão exclusivamente para utilizar a VPN com dispositivos fornecidos pelo **Grupo CPFL**;
- Para utilização do sistema de acesso remoto o colaborador deverá possuir usuário de rede para acesso à rede do **Grupo CPFL**;
- O usuário de rede não poderá estar bloqueado ou inativo;


7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Políticas e Diretrizes de Gestão	Eletrônico: Portal Multi > Portais > Sistemas de Gestão> Sistemas de Gestão - Home	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8. ANEXOS

Nada a considerar

N.Documento: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 5 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------

	Tipo de Documento: Procedimento
	Área: EIS-GERENCIA DE SEGURANCA DE TI
	Título do Documento: Procedimento de Acesso Remoto

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Rocha

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não Aplicável	Não Aplicável	Documento em versão inicial
1.0	29/04/2022	Inclusão da Definição "Grupo CPFL"
1.1	06/05/2022	Inclusão de uma premissa para utilizar VPN

N.Documento: 18893	Categoria: Tático	Versão: 3.0	Aprovado por: Emerson Cardoso	Data Publicação: 03/12/2023	Página: 6 de 6
-----------------------	----------------------	----------------	----------------------------------	--------------------------------	-------------------