 <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – Azure Active Directory
	Directory	

Sumário

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

1.OBJETIVO

Este documento tem por objetivo estabelecer parâmetros e especificações técnicas para a aplicação Azure AD no ambiente Office 365.

2.ÂMBITO DE APLICAÇÃO

2.1.Empresa

Todas as empresas do Grupo CPFL Energia.

2.2.Área

Todas as áreas de negócio das empresas do Grupo CPFL Energia.

3.DEFINIÇÕES

Não aplicável.


4.DOCUMENTOS DE REFERÊNCIA

Diretrizes Corporativas de Segurança da Informação (GED14369).

5.RESPONSABILIDADES

Não aplicável.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18724	Instrução	1.0	Emerson Cardoso	27/05/2021	1 de 3


 CPFL ENERGIA <i>Uso Interno</i>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – Azure Active Directory
	Directory	

6. REGRAS BÁSICAS

Na tabela abaixo encontram-se os requisitos de segurança para o Azure Active Directory:

Requisitos	Porque	Para quem
Autenticação de múltiplo fator para usuários em roles de administração	Melhoria de segurança para autenticação no Azure	Todas as funções/roles de Administrador
Autenticação de múltiplo fator para todos os usuários	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Devem estar designados entre 2 e 4 administradores globais	Para que seja possível realização de auditorias entre os administradores, além disso caso um administrador esteja ausente, há outro para suporte	Administradores Globais
O serviço de redefinição de senha de autoatendimento seja habilitado com MFA, exceto para contas de administradores.	Para alterar o método atual de auto reset de senha, e desafogar o HelpDek.	Para todos os usuários
A proteção de senha do Azure Active Director deverá estar habilitada	Melhoria de segurança para autenticação no Azure	Para todos os usuários
As políticas de Conditional Access para bloquear protocolos legados (que não exigem autenticação MFA)	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Sincronização do Hash de senha esteja habilitada para detecção de vazamento de credencial	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Proteção de identidade ativada para identificar comportamento de logon	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Habilitar políticas de sing-in-risk do Azure AD Identify Protection	Proteger contra riscos de segurança nos logons no Azure	Para todos os usuários
Habilitar políticas de user risk do Azure AD Identify Protection	Proteger contra riscos de segurança nos logons no Azure	Para todos os usuários
Use o acesso privilegiado Just In Time para funções do Office365(JIT) - Não está no escopo	Proteger contra riscos de segurança nos logons no Azure	Todas as funções/roles de Administrador
Habilitar autenticação moderna para o Exchange Online. - Dentro da sua aplicação	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Habilitar autenticação moderna para o Teams - Dentro da sua aplicação	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Habilitar autenticação moderna para o SharePoint - Dentro da sua aplicação	Melhoria de segurança para autenticação no Azure	Para todos os usuários
Garantir que haja troca periódicas de senhas de acordo com as regras da CPFL	Atender políticas de CPFL	Para todos os usuários

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18724	Instrução	1.0	Emerson Cardoso	27/05/2021	2 de 3

 Uso Interno	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – Azure Active Directory
	Directory	

Criar contas de acesso de emergência e não devem ser atribuídas a indivíduos específicos.	Para que em casos de emergências não ficar sem acesso no Azure	Administrador Global
Ativar search do audit log no Microsoft 365	Para análise de problemas e tratamento de incidente	Administrador Global e time da segurança da informação
Garantir que os Resource Locks estão definidos para recursos críticos do Azure.	Melhorar as boas práticas de segurança	Para todos os usuários

7.CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Requisitos de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8.ANEXOS

Não aplicável.

9.REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Ana Maria Leite Felix Pelepka

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não aplicável	Não aplicável	Documento em versão inicial

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18724	Instrução	1.0	Emerson Cardoso	27/05/2021	3 de 3