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

## 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.....	6
8.	ANEXOS.....	6
9.	REGISTRO DE ALTERAÇÕES .....	6

### 1.OBJETIVO

Este documento tem por objetivo estabelecer parâmetros e especificações técnicas para a aplicação Sharepoint 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:
18712	Instrução	1.0	Emerson Cardoso	27/05/2021	1 de 7

 <b>Uso Interno</b>	Tipo de Documento:	Especificação Técnica
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança da Informação – Sharepoint

## 6. REGRAS BÁSICAS

Na tabela abaixo encontram-se os requisitos de segurança para o Sharepoint.


Requisitos	Usuário restrito	Usuário adm	Usuário executivo	Prestador	Exceção	Porque
Acessar com MFA	sim	sim	sim	sim	NA	Melhorar as boas práticas de segurança da informação
Device corporativo com MDM	sim	sim	sim	sim	NA	Restringir acesso somente aos colaboradores para evitar acesso indevido e vazamento de informações
Mobile com MDM	sim	sim	sim	sim	NA	Restringir acesso somente aos colaboradores para evitar acesso indevido e vazamento de informações
Compartilhar arquivo dentro Org.	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Compartilhar arquivo fora Org.	não	sim	sim	não	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Configurar acesso condicional para garantir que dispositivos conectados ao Sharepoint devem atender aos requisitos de segurança e conformidade, em dispositivos gerenciados.	sim	sim	sim	sim	NA	Melhorar as boas praticas de segurança da informação
Exigir que todo arquivo compartilhado externo tenha fluxo de aprovação do	NA	sim	não	NA	NA	Proteger contra acesso indevido e vazamento de informações confidenciais

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18712	Instrução	1.0	Emerson Cardoso	27/05/2021	2 de 7

gerente.						
Colocar como desativada a permissão padrão de editar arquivos ao fazer compartilhamentos.	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Garantir que os arquivos salvos no Sharepoint sejam ativados por padrão permissão somente ao proprietário	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Para compartilhamento de arquivos confidenciais, ativar para escolher pessoas específicas ou pessoas da área, e não todos na organização.	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Notificar quando ocorrer compartilhamento externo.	NA	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Notificar sobre acesso aos seus dados	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Ativar exigência de uma data de expiração no link de compartilhamento externo da organização.	NA	não	sim	não	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Possibilitar pesquisas restritas por grupo de usuários e/ou departamentos.	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Ativar O365 ATP SafeLinks para todos Office Apps.	sim	sim	sim	sim	NA	Proteger contra malwares e ameaças avançadas

Ativar o Office 365 ATP para todos Office Apps.	sim	sim	sim	sim	NA	Proteger contra malwares e ameaças avançadas
Garantir que os arquivos perigoso do Office 365 SharePoint e OneDrive não sejam permitidos para download.	.jar .avi .bat .chm .cmd .dll .exe .hta .js .jse .lnk .mov .wma .vxd .vbs .vbe .shs .mpeg .mpg .pif .scr .shm .wmv .mp3 .mp4 .zip .rar .7z .os2 .w16 .dos .com .pif .rar					Proteger contra malwares e ameaças avançadas
Ativar criptografia no dispositivos móveis quando utilizar o mobile app do Sharepoint.	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Garantir que seja protegido e monitorado pelas ferramentas de segurança DLP, ATP, Cloud App Security, SIEM.	sim	sim	sim	sim	NA	Proteger contra malware, ameaças avançadas e dados confidenciais
DLP/Bloquear dados pessoais	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Classificação da informação e label	sim	sim	sim	sim	NA	Proteger contra acesso indevido e vazamento de informações confidenciais
Garantir que o consentimento do usuário para que os aplicativos acessem os dados da empresa em seu nome não seja	sim	sim	sim	sim	NA	Melhorar as boas praticas de segurança da informação

permitido.						
Ativar o workflow do consentimento do administrador.	sim	sim	sim	sim	NA	Melhorar as boas praticas de segurança da informação
Garantir que todo arquivo armazenado e trafegado seja criptografado.	sim	sim	sim	sim	NA	Evitar vazamento de informações
Garantir que haja notificações de segurança para todo comportamento suspeito ou anormal.	sim	sim	sim	sim	NA	Proteger contra malware, ameaças avançadas e dados confidenciais
Desativar acesso anônimo nos sites.	sim	sim	sim	sim	não	Proteger contra acesso indevido e vazamento de informações confidenciais
Bloquear compartilhamento de informações com outros departamentos	sim	sim	não	sim	não	Proteger contra acesso indevido e vazamento de informações confidenciais
Limitar tamanho do upload para arquivos	10GB	10GB	10GB	10GB	250GB	Proteger contra acesso indevido e vazamento de informações confidenciais
Download pro device corporativo, com MDM	sim	sim	sim	sim	NA	Evitar vazamento de informações
Ativar auditoria para rastreabilidade	sim	sim	sim	sim	NA	Proteger contra malware, ameaças avançadas e dados confidenciais
Restaurar arquivo no histórico da atividade do arquivo	90 dias	90 dias	90 dias	90 dias	NA	Proteger contra malware, ameaças avançadas e dados confidenciais

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

Recuperar arquivo após excluído da Lixeira	90 dias	90 dias	90 dias	90 dias	NA	Proteger contra malware, ameaças avançadas e dados confidenciais
Bloquear limpar lixeira	sim	sim	sim	sim	NA	Proteger contra malware, ameaças avançadas e dados confidenciais
Integrações com app/bot	não	não	não	não	sim	Proteger contra malware, ameaças avançadas e dados confidenciais

## 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
-----------------	-------------------------	---

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18712	Instrução	1.0	Emerson Cardoso	27/05/2021	6 de 7

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

Não aplicável	Não aplicável	Documento em versão inicial
---------------	---------------	-----------------------------

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18712	Instrução	1.0	Emerson Cardoso	27/05/2021	7 de 7