
 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Checklists de Segurança para Avaliação de Terceiros

## Sumário

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

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18825	Instrução	1.0	Emerson Cardoso	25/06/2021	1 de 6

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Checklists de Segurança para Avaliação de Terceiros

## 1. OBJETIVO

Este Procedimento tem como objetivo estabelecer os itens mínimos de Segurança requeridos para avaliação de terceiros e prestadores de serviços, baseando-se nos riscos avaliados relacionados a fornecedores e prestadores de serviço do **Grupo CPFL Energia**.

## 2. ÂMBITO DE APLICAÇÃO

### 2.1. Empresa

Esta norma é aplicável ao **Grupo CPFL Energia** e a todas as suas controladas diretas e/ou indiretas, excetuadas as empresas com modelo de gestão e governança próprio.


### 2.2. Área

Todas as áreas do **Grupo CPFL Energia**.

## 3. DEFINIÇÕES

- **CRM DYNAMICS:** Ferramenta utilizada para registro das Ocorrências.
- **PORTAL DE SERVIÇOS:** Ferramenta para registro de Ocorrências no CRM Dynamics. O acesso se dá via intranet da CPFL;
- **USUÁRIO:** Nome atribuído à pessoa que executa alguma atividade nos sistemas da CPFL. Todo usuário possui um ID de identificação para acesso aos sistemas;
- **CONFIDENCIALIDADE:** É a garantia de que a informação é acessada somente por usuários com o devido direito. Está diretamente vinculada a proteção da privacidade dos usuários e suas informações.
- **DISPONIBILIDADE:** É a garantia de que a informação está disponível para o usuário (que tem tal direito de acesso) e para o sistema de informação no momento que o usuário necessita consumi-la.
- **TERCEIRO/PRESTADOR DE SERVIÇOS:** É a um funcionário, vários e /ou uma empresa, ou comunidade que executa uma ou mais atividades econômicas intangíveis, que não assumem a forma de um produto e/ou mercadoria, e inseparáveis, em outras palavras que é produzida e consumida ao mesmo tempo.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18825	Instrução	1.0	Emerson Cardoso	25/06/2021	2 de 6

 Confidencialidade	Tipo de Documento: Formulário
	Área de Aplicação: Segurança da Informação
	Título do Documento: Checklists de Segurança para Avaliação de Terceiros

#### 4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- Política de Segurança da Informação do **Grupo CPFL Energia**;
- Norma de Classificação da Informação do **Grupo CPFL Energia**;
- Norma de Gestão de Terceiros do **Grupo CPFL Energia**;
- Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL Energia**.

#### 5. RESPONSABILIDADES

- **Contratante**

Aplicar este procedimento e averiguar periodicamente se tanto o contrato quanto os serviços prestados pelo terceiro atendem os itens abordados neste documento.

- **Terceiro/Prestador de Serviços**

Cumprir os itens mencionados neste procedimento bem como gerar evidências dos itens apontados como em conformidade.

#### 6. REGRAS BÁSICAS

O terceiro e/ou prestador de serviços deverá estar em conformidade com os itens abaixo, permitindo auditoria sempre que requerido e gerando evidências para comprovar a aderência com o Checklist.


##### Público-alvo

Terceiros ou prestador de serviços do **Grupo CPFL Energia** que tenha necessidade acesso a utilização da infraestrutura, sistemas computacionais ou processar informações do **Grupo CPFL Energia**.

##### 6.1 Infraestrutura física

- ✓ A empresa dispõe de recepção ou portaria que solicite a identificação de funcionários e/ou terceiros. [ ]
- ✓ O acesso ao local é realizado via utilização de crachá eletrônico ou outro meio de identificação. [ ]

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18825	Instrução	1.0	Emerson Cardoso	25/06/2021	3 de 6

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Checklists de Segurança para Avaliação de Terceiros


- ✓ O local possui alarmes contra roubo (Arrombamento e/ou Sensor de Presença).  
[ ]
- ✓ O local possui segurança 24 horas e com ronda em turnos pré-determinados.  
[ ]
- ✓ Existem políticas de segurança para utilização do crachá, contemplando obrigatoriedade de uso, estar em local visível, bem como outros itens. [ ]

## 6.2 Infraestrutura física Data Center

- ✓ O Data Center possui sistema exclusivo de ar-condicionado. [ ]
- ✓ O Data Center possui contingência para o sistema de ar-condicionado. [ ]
- ✓ O Data Center possui equipamentos de controle de temperatura. [ ]
- ✓ O Data Center possui processo formal de acesso às áreas críticas. [ ]
- ✓ O Data Center possui equipamento de controle de acesso. [ ]
- ✓ O Data Center possui câmera de segurança interna. [ ]
- ✓ O Data Center possui nobreak para os equipamentos considerados críticos. [ ]
- ✓ O Data Center possui gerador de energia que suporte uma ou mais operações contratadas. [ ]
- ✓ O Data Center possui um processo de manutenção e testes do(s) gerador(es).  
[ ]

## 6.3 Controle de Acesso


- ✓ A empresa dispõe de procedimentos e/ou sistemas para gerenciamento de contas de usuários e sistemas, incluindo troca regulares de senhas. [ ]

 Confidencialidade	Tipo de Documento:	Formulário
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Checklists de Segurança para Avaliação de Terceiros

- ✓ Existe uma política que bloqueie criação de usuário genérico, além da troca de senhas padrão. [ ]
- ✓ O acesso administrativo nos laptops e/ou servidores estão amparados por justificativa de uso para o negócio. [ ]
- ✓ É disponibilizado ao funcionário equipamento corporativo para o trabalho consultivo e/ou remoto. [ ]
- ✓ Existe um segundo fator de autenticação para acesso remoto. [ ]

#### 6.4 Gestão de Segurança da Informação

- ✓ [ ] Caso haja subcontratação de serviços, isso deverá estar explícito;
- ✓ [ ] Ainda sobre subcontratação de serviços, o terceiro e/ou prestador de serviços deverá obter o consentimento formal da organização e uma descrição dos controles deve ser preenchida pelos subcontratados;
- ✓ [ ] O terceiro ou prestador de serviços deverá dispor de uma Política de Segurança da Informação, documentada e publicada a nível organizacional;
- ✓ O terceiro ou prestador de serviços deverá dispor de documentos que suportem Política de Segurança da Informação:
  - [ ] Classificação da Informação;
  - [ ] Utilização de recursos de rede e computacionais;
  - [ ] Controle de Acesso e limitação de uso;
  - [ ] Acordo de Confidencialidade (NDA = Non Disclosure Agreement)
  - [ ] Treinamento e Conscientização de Segurança da Informação
- ✓ [ ] O terceiro ou prestador de serviços deverá dispor e assegurar, se pertinente, controles para proteger a integridade, a disponibilidade e a confidencialidade das informações;
- ✓ [ ] O terceiro ou prestador de serviços deverá dispor e assegurar, se pertinente, controles para garantir a devolução ou destruição dos ativos de informações após seu uso e controles para impedir a cópia e distribuição das informações;

 <b>CPFL</b> <b>ENERGIA</b> Confidencialidade	Tipo de Documento: Formulário
	Área de Aplicação: Segurança da Informação
	Título do Documento: Checklists de Segurança para Avaliação de Terceiros

- ✓ [ ] O terceiro ou prestador de serviços deverá dispor e assegurar, se pertinente, certificações dos profissionais envolvidos na prestação de serviço, bem como da empresa se exigido;
- ✓ [ ] O terceiro ou prestador de serviços deverá disponibilizar as evidências contratuais e legais no que tange Recursos Humanos sobre os recursos contratados de forma temporário ou indeterminada;
- ✓ [ ] O terceiro ou prestador de serviços deverá permitir auditorias por parte do contratante ou de empresa a definida pelo contratante sobre itens pertinentes ao contrato e/ou prestação de serviços;

## 7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Norma 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