 Uso Interno CPFL	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades
Uso Interno		

Sumário

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

1. OBJETIVO

Este procedimento apresenta o modo como a CPFL deve proceder para a realização e identificação das necessidades de análises de vulnerabilidades e das possíveis correções necessárias para estas e fornecer informações de como elaborar o escopo para as análises de vulnerabilidades, executadas semanalmente, quinzenalmente ou mensalmente.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas do **Grupo CPFL**.

2.2. Área

Todas as áreas do **Grupo CPFL**.

3. DEFINIÇÕES

Segurança da Informação: proteção dada às informações e ativos de informação;


Ativo de informação: processos, pessoas, tecnologia e ambientes que interagem com a informação durante qualquer fase do seu ciclo de vida;

Incidente de Segurança da Informação: qualquer evento que possa comprometer a Segurança da Informação.

Colaborador: empregados, estagiários, consultores, fornecedores ou convidados que usam ou têm acesso as instalações do **Grupo CPFL Energia**.

Riscos: incerteza sobre o atingimento de objetivos;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	1 de 7

 Uso Interno CPFL	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades
Uso Interno		

Vulnerabilidade: comportamento funcional de um produto ou serviço que viole regra(s) de segurança implícita ou explícita;

Ameaça: potencial causa de um incidente indesejado, que pode resultar em danos a um sistema ou organização;

Probabilidade: chance de algo acontecer;

Mitigação de risco: ato de reduzir ou minimizar a ocorrência de um risco;

Patches: conjunto de configurações e parâmetros sistêmicos a ser implementado em sistemas de informação;

Ambiente de produção: ambiente tecnológico aos quais processos de negócios são executados através de sistemas de informação.

Exploit: parte do software criados por crackers para comprometer funcionamento normal do ativo de informação;

Negação de serviço: indisponibilidade do serviço causada por sobrecarga através de inúmeras requisições;

Vazamento de informação: acesso a informações não autorizadas;

Crackers: pessoas com conhecimento avançado em tecnologia da informação que utilizam do conhecimento para realizar ações não autorizadas ou ilegais;

Hardening: procedimento de implementação de controles de segurança visando reduzir vulnerabilidades e riscos de ativos de informação.

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.

VM = Vulnerability Management

WAS = Web Application Scanning

DT = Datacenter

CRM = Customer Relationship Management


4. DOCUMENTOS DE REFERÊNCIA

Internos –

Diretrizes de Segurança da Informação CPFL – nº 14369

Norma de Gestão de Vulnerabilidades – nº 18895

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	2 de 7

 Uso Interno CPFL Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades

Procedimento de Análise de Risco do SGSI – nº 14367

Externos –

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação

ABNT NBR ISO/IEC 27032:2013 – Tecnologia da Informação – Técnicas de segurança –

5. RESPONSABILIDADES

Área de Segurança da Informação

- Executar todas as atividades inerentes ao ciclo de tratamento de vulnerabilidades;
- Engajar as áreas responsáveis pelas correções no tratamento tempestivo das vulnerabilidades
- Identificar novas ameaças, monitorar as existentes, e fazer o acompanhamento das correções
- Atualizar este documento sempre que aplicável.
- Realizar e acompanhar os testes de vulnerabilidades

Áreas de TI responsáveis pelos ativos e sistemas

- Promover correção das vulnerabilidades indicadas pelas varreduras e testes
- Atuar preventivamente no combate às vulnerabilidades
- Solicitar testes e scans de ameaças quando das mudanças nos ativos e sempre que um ativo for colocado em produção
- Atuar tempestivamente de acordo com os prazos estabelecidos nesta norma

6. REGRAS BÁSICAS


6.1. Realização das análises de vulnerabilidades

As análises de vulnerabilidades devem ser realizadas pelas ferramentas Rapid7 de propriedade da área de Tecnologia da Informação da CPFL, conforme cronograma definido são realizados testes e varreduras no ambiente para identificar, analisar, tratar, reportar, monitorar e priorizar as vulnerabilidades continuamente.

Semanalmente serão analisados com escopo de servidores e quinzenal/mensalmente serão analisados o escopo de aplicação.

Análises pontuais ou emergenciais poderão ser realizadas e sempre que houver necessidade será efetuada uma reanálise.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	3 de 7

 Uso Interno CPFL Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades

6.2. Classificação das vulnerabilidades quanto à criticidade

São definidos os seguintes níveis de classificação das vulnerabilidades de acordo com seus impactos:

Critical

Representam as maiores falhas de segurança, que poderão conduzir efeitos como: criação, modificação, remoção, alteração de informações, acesso especial ao banco de dados, ataques aos mecanismos de defesa, elevação de privilégios, etc.

As consequências são extremamente críticas e podem causar grandes danos ao ambiente ou roubo de informações confidenciais. A característica principal deste tipo de vulnerabilidade é que esta pode ser explorada por meio de “exploits” disponibilizados na internet através de boletins de segurança e, portanto, de fácil exploração.

Ações imediatas precisam ser realizadas para corrigir as vulnerabilidades nos sistemas afetados. Neste caso pode-se ainda considerar uma revisão da segurança de toda a arquitetura, sistemas e processos interligados ao sistema afetado.

Severe

Representam as falhas de segurança que podem causar diversos comprometimentos à segurança, podendo conduzir a efeitos como “negação de serviço”, vazamento de informações internas, acesso especial a arquivos ou banco de dados com informações internas, desinformação, leitura e criação de informações internas, etc.

Ações corretivas devem ser tomadas para eliminar as vulnerabilidades nos serviços afetados para garantir o nível de segurança.

Moderate


Representam as falhas de segurança menores como: leitura de informações (não confidenciais) dos recursos, vazamento de informações.

Estas vulnerabilidades podem causar danos potenciais se exploradas em conjunto. Normalmente são exploradas por Crackers experientes com muitos recursos à sua disposição procuram aproveitar-se do baixo nível de exposição.

A ameaça à segurança é menor, no entanto, ações corretivas devem ser tomadas para favorecer o aumento do nível de arquitetura de segurança alinhando assim com as melhores práticas corporativas.

As ferramentas Rapid7 possui as seguintes classificações de severidade (que segue a classificação da CPFL:

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	4 de 7

 Uso Interno CPFL CPFL ENERGIA Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades

Severidade (CVSS)	Classificação CPFL
0 to 3.4	Moderate
3.5 to 7.4	Severe
7.5 to 10	Critical

6.3. Tratamento das vulnerabilidades identificadas

Todas as vulnerabilidades identificadas deverão ser tratadas o mais breve possível, salvo as situações em que não haja tratamento o motivo deverá ser justificado.

Os prazos recomendados para tratamento dependem da criticidade da(s) vulnerabilidade(s) associada(s) como apresentado a seguir:

Criticidade	Prazo
Critical	30 dias
Severe	60 dias
Moderate	90 dias

Após a geração do Relatório de Vulnerabilidades a área de TI deve abrir um chamado no CRM Dynamics.

O controle do tratamento das vulnerabilidades será realizado através de planilha específica.


Os casos de vulnerabilidade identificados, analisados e tratados são direcionados à equipes responsáveis pela remediação, para documentar/evidenciar a correção ou justificar a impossibilidade de correção, com a devida criticidade estabelecida.

6.4 Descrição do Processo

01 Ciclo semanal scans (para servidores)

01 Ciclo de mensal/quinzenal scans (para aplicações)

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	5 de 7

 Uso Interno CPFL CPFL ENERGIA Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades

Atividade	Tipo	Descrição
Criação, Alteração e Exclusão de Usuário das ferramentas Rapid7	Solicitação	Mediante solicitação, poderão ser criados, alterados ou excluídos os usuários para acesso ao Rapid7, com acesso aos relatórios.
Varredura de Vulnerabilidades em Servidores	Rotina	Semanalmente será realizada a varredura na rede, identificando as vulnerabilidades existentes em servidores. As varreduras realizadas serão baseadas nas categorias de testes automatizados. Será feita com base na ferramenta: IVM.
Varredura de Vulnerabilidades em Aplicações	Rotina	Quinzenal/Mensalmente será realizada o scan de vulnerabilidade nos principais sites do Grupo CPFL . Será feita com base na ferramenta: AppSec.

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 se aplica.

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Rocha

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	6 de 7

 Uso Interno CPFL Uso Interno	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Gestão de Vulnerabilidades

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	02/06/2022	Revisão geral do documento
1.1	22/08/2022	Atualização da ferramenta, anteriormente AppSpider, agora AppSec

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18897	Instrução	1.3	Emerson Cardoso	31/08/2022	7 de 7