 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO.....	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA.....	4
5.	RESPONSABILIDADES.....	4
6.	REGRAS BÁSICAS.....	4
7.	CONTROLE DE REGISTROS.....	16
8.	ANEXOS.....	17
9.	REGISTRO DE ALTERAÇÕES.....	17

1.OBJETIVO

A CPFL vem através desta normativa apresentar os requisitos de Segurança cibernética de fornecimento da Infraestrutura de Rede das Subestações do **Grupo CPFL**.

2.ÂMBITO DE APLICAÇÃO

2.1. Empresa

Distribuidoras do Grupo CPFL Energia.

2.2. Área

Segurança da Informação, Engenharia, Fornecedores, Serviço de Transmissão, Gestão de Ativos e Operação.

3.DEFINIÇÕES

Para simplificação de entendimento e de texto, os termos e siglas a seguir listados, constantes desta Especificação, cujos significados não forem explicitamente declarados, devem ser assim entendidos:


3.1. SE

Subestação Distribuidora Padrão, objeto do Fornecimento.

3.2. SSD

Sistema Secundário Digital: Representa o sistema de proteção e controle digitalizado, com todo o hardware e software necessário, plenamente integrado e operacional, na configuração e funcionalidade especificadas para cada SE.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	1 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

3.3. Controle

Entende-se por controle os comandos pontuais ou recorrentes, manuais ou automáticos, locais ou remotos, com seus intertravamentos e sinalizações. Inclui-se também supervisão do processo via medição, indicações, sinalizações, alarmes e eventos associados ao estado e operação dos equipamentos controlados.

3.4. Proteção

Entende-se por proteção a ação do SSD em resposta a distúrbios, perturbações, defeitos ou falhas, internos ou externos a SE e/ao SSD, com seus registros de oscilografia, alarmes, eventos e outros diagnósticos associados.

3.5. Monitoramento

Entende-se por monitoramento ações específicas de supervisão cíclicas ou contínuas com respectivos diagnósticos da operação dos equipamentos e unidades do SSD.

3.6. UTR

Unidade Terminal Remota.

3.7. Dispositivos

São os IEDs, Intelligent Electronic Devices, de nível de vão, isto é, dispositivos numéricos integrados de proteção e controle, microcomputadores, periféricos, hubs, concentradores, anunciadores, UTR's e demais dispositivos digitais devidamente montados em suas caixas, e aptos para instalação em painéis e equipamentos, para perfeita operação. Compõem-se de hardware e facilidades de configuração, diagnósticos e análise de sua operação via software.

3.8. Módulos

São todas as partes individuais componentes dos dispositivos, isto é, fontes, placas de entrada e saída, de comunicação, conversores etc., extraíveis ou não. Compõem-se de hardware e, eventualmente, parametrizações básicas de software.

3.9. Componentes

São os demais componentes secundários integrantes dos módulos, dos dispositivos, dos painéis etc., isto é, relés auxiliares, blocos de teste, plugs, chaves, botoeiras, conectores, jumpers, adaptadores, ativos ou não, cabos, blocos de teste, enfim toda a miscelânea necessária à operação normal do SSD, ao longo de sua vida útil.

3.10. UA

Unidade Autônoma: são dispositivos de nível de vão, que operam de maneira autônoma sobre o processo, perfazendo plenamente a funcionalidade no nível de vão.


3.11. LAN

Local Area Network: Rede de comunicação serial local.

3.12. CTR

Concentrador: Dispositivo ou subsistema para interconexão entre o nível de vão e de SE. Pode ser uma UTR, Hub ou outro ente de funcionalidade híbrida e/ou similar. A utilização de microcomputadores tipo PC não será aceita para essa funcionalidade.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	2 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

3.13. SOL

Subsistema de Operação Local: Arranjo de dispositivos que permitem a plena operação local da SE e demais funcionalidades de tempo real aqui especificadas. Compõe-se de seus dispositivos principais e periféricos necessários à sua finalidade.

3.14. SMAL

Subsistema de Monitoramento e Análise Local: Arranjo de dispositivos que permitem localmente o armazenamento de dados históricos, monitoramento local e remoto da proteção, e demais funcionalidades de análise e apoio à engenharia e áreas corporativas da CPFL. Compõe-se de seus dispositivos principais e periféricos necessários à sua finalidade.

3.15. SMAR

Subsistema de Monitoramento e Análise Remoto: Arranjo de dispositivos que acessam remotamente e armazenam dados históricos, monitoramento da proteção, e demais funcionalidades de análise e apoio à engenharia e áreas corporativas da CPFL. Compõe-se de seus dispositivos principais e periféricos necessários à sua finalidade.

3.16. SPC

Subsistema de Processamento Central: Subsistema que integra física e funcionalmente o SMAL, SOL e CTR, perfazendo plenamente a funcionalidade centralizada da SE.

3.17. CO

Centro de Operação: É o Sistema de Telecontrole da CPFL. Trata-se do centro integrado de operação da CPFL, que unifica o CO, Centro de operação de Área, e o COD, Centro de Operação da Distribuição.

3.18. SPR

Subsistema de Processamento Remoto: Subsistema que integra física e funcionalmente o SPC ao CO, perfazendo plenamente a funcionalidade remota da SE, conforme aqui especificado.

3.19. TAF

Teste de Aceitação de Fábrica.

3.20. TAC

Teste de Aceitação de Campo ou Comissionamento.

3.21. Elementos Funcionais

São módulos, componentes e software de parametrização que realizam funções de proteção e controle, alimentação auxiliar, comunicação e aquisição de dados no âmbito das UAs e CTR.

3.22. ED, EA e SD

Respectivamente, entrada digital, entrada analógica e saída digital.


3.23. Software Básico

Software inerentes dos dispositivos e módulos para seu funcionamento default.

3.24. Linguagens de Programação

Ferramentas de alto nível, padronizadas ou proprietárias, destinadas à codificação dos

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	3 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

programas para implementação das funções.

3.25. Aplicativos

Software padronizado ou proprietário usado para configurar, parametrizar, tratar dados, analisar desempenho e executar atuações das UAs, CTR, SOL, SMAL e SMAR.

3.26. Parametrizações

Configurações das UAs, CTR, SOL, SMAL e SMAR, confecção de IHM, customização de tabelas etc., para o funcionamento básico destas unidades nos seus respectivos níveis.
Especificação Técnica

4. DOCUMENTOS DE REFERÊNCIA

Interno

GED 6204 - Sistema Secundário Digital para Subestações de Distribuição da CPFL;

Externo

Cisco Cyber Vision Architecture Guide

Cisco Catalyst IE3400 Rugged Series

Cisco Secure Firewall ISA3000

5. RESPONSABILIDADES

Arquitetura: Encaminhar para os fornecedores os requisitos de segurança que devem ser seguidos na criação de novas subestações.

Segurança da Informação: Apoiar em assuntos técnicos envolvendo segurança cibernética para atendimento dessa norma.

Fornecedor: Atender, implementar, configurar todos os requisitos envolvidos nessa norma.

6. REGRAS BÁSICAS


Os fornecedores devem envolver os serviços, produtos e arquitetura.

Serviço de instalação dos dispositivos, ativação, configuração e integração com o Cisco CyberVision (No caso do IE3400 - Switch Cisco)

Serviço de instalação dos dispositivos, ativação, configuração e integração com o Cisco FDM e Cisco Cybervision (No caso do IC3000 - Firewall)

À CPFL, busca parceiros tecnológicos para o fornecimento de firewalls e switches de linha Industrial, próprios para o funcionamento em Subestações de Energia com toda a camada de Gerenciamento de um único Fabricante possibilitando a CPFL ter gerência completa, centralizada e focada em produtos e redes de dados do setor. Os fornecedores devem implementar os itens que serão descritos abaixo, seguem;

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	4 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

- Permitir a visibilidade em Sistemas de Controle Industrial (ICS) para inventariar e desenvolver linhas de base para dispositivos, aplicativos e perfis de tráfego;
- Pontos de contato seguros onde as pessoas e seus dispositivos interagem com o ICS;
- Adicionar ferramentas que permitam e informem uma resposta rápida a incidentes;
- Preparar para a mudança inevitável de componentes de Tecnologia Operacional (OT) migrando para a nuvem;
- Alinhar com os padrões de segurança da indústria, como NERC CIP e NIST

O objetivo fundamental para aplicar a segurança cibernética a ativos de serviços públicos é permitir a visibilidade em ambientes críticos de ICS e de controle de supervisão e aquisição de dados (SCADA). Essa visibilidade fornece aos operadores de segurança os dados necessários para compreender a linha de base do sistema para dispositivos, aplicativos e tráfego. Essas linhas de base são críticas e formam a base para a identificação de anomalias que resultam de invasões cibernéticas por malware, worms, vírus e outras explorações do sistema. Os produtos necessários para composição dessa Infraestrutura e que deverão permitir visibilidade em tempo real e detecção de anomalias são:

- Software para gestão, visibilidade do tráfego de rede com os protocolos específicos do setor;
- Firewalls;
- Gateways;
- Ferramenta para Network Analytics;
- Switches Industriais Ethernet (IE) com NetFlow;
- Inspeção profunda de pacotes para IEC 61850, IEC 101/104, Modbus, Ethernet / IP e Protocolo de rede distribuída 3 (DNP3)

Os recursos de cyber segurança deve ser mapeados diretamente para os padrões de cyber segurança industrial, como:

- NERC CIP
- EU NIS
- ISA-99 / IEC62443
- NIST


Pontos Chaves para Infraestrutura

→ **Gerenciamento:** Ferramenta de gerenciamento intuitiva para nos ajudar a implantar, monitorar e gerenciar com eficiência um grande número de dispositivos, serviços de rede e VPNs para que a rede seja construída para durar e com escalabilidade.

→ **Automação e Rede de Subestação:** A atualização de subestações com Ethernet e IP IEC61850 e SCADA habilitam funções de controle e proteção com base em mais troca de dados entre IEDs, RTUs e outros dispositivos. Reduzir significativamente os períodos de construção e auditoria, simplificar a solução de problemas ao permitir um tempo de valorização mais rápido. A arquitetura deve incluir IEC 61850, redundância de rede (PRP, HSR), temporização e sincronização (PTP) e segurança.

Criar uma rede eficaz para conectar subestações de transmissão e distribuição à matriz e

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	5 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

ao data center.

Isso possibilitará uma série de serviços automatizados que nos permitirá monitorar dispositivos eletrônicos inteligentes (IEDs), coletar leituras de sensor, gerenciar ativos e provisionar dispositivos e software para operação e SCADA não operacional, sincrofases, CRAS, teleproteção e segurança física.

→ **Segurança de Rede:** Medidas de segurança reforçadas para proteger de ataques cibernéticos e uma arquitetura holística de segurança cibernética para subestações e redes de distribuição. Podendo identificar e rastrear dispositivos e protocolos de OT na rede, em direção à conformidade de segurança, detecção, mitigação de ameaças e possuir um mapa dos produtos de segurança para os requisitos NERC CIP.

Os Firewall (IPS) e Switch (IDS) devem ser compatíveis com o **Cisco Cyber Vision**.

6.1. ESCOPO DO PROJETO

À integradora de soluções fim a fim, deve oferecer à CPFL Energia escopo de fornecimento de equipamentos e serviços para Implementação da Rede das Subestações considerando equipamentos, licenciamentos, softwares e serviços Cisco, solução completa de um único fabricante.


6.2. ESPECIFICAÇÃO DA GARANTIA

A garantia dos Firewalls e Switches das Subestações fornecidos pela Cisco, deverá ser de 60 meses do tipo 8x5xNBD, exceto para os componentes do Cyber Vision que deverá ser de 24x7x4.

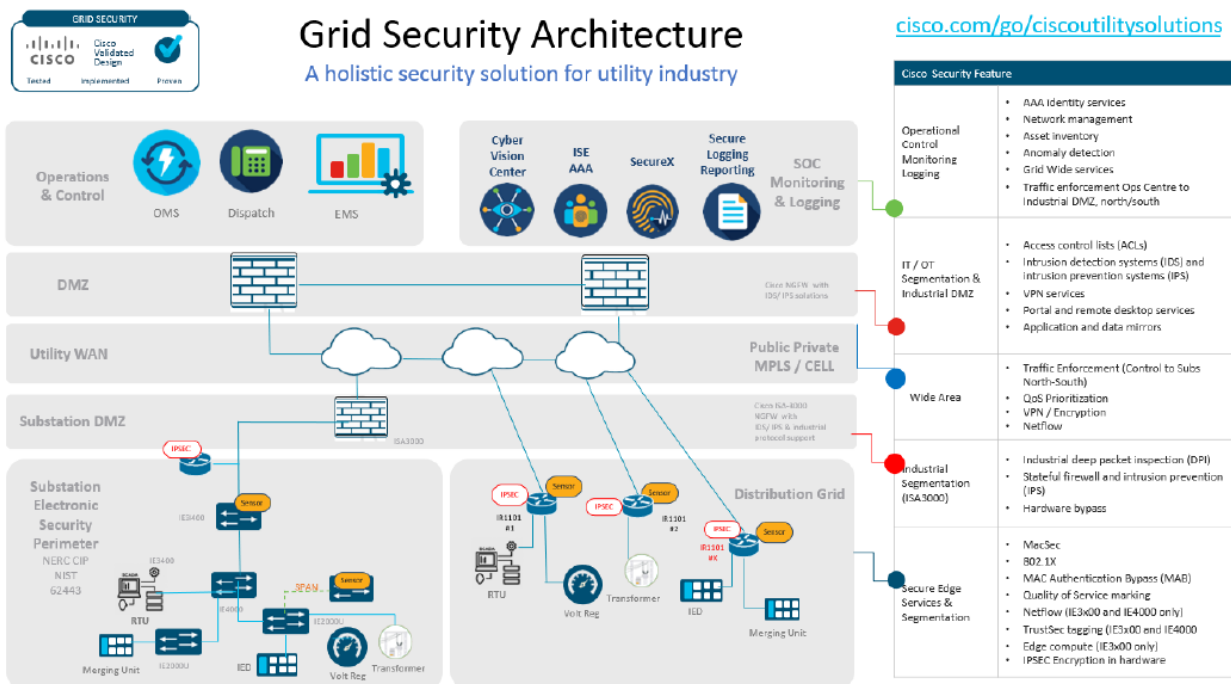
6.3. EQUIPAMENTOS

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	6 de 17

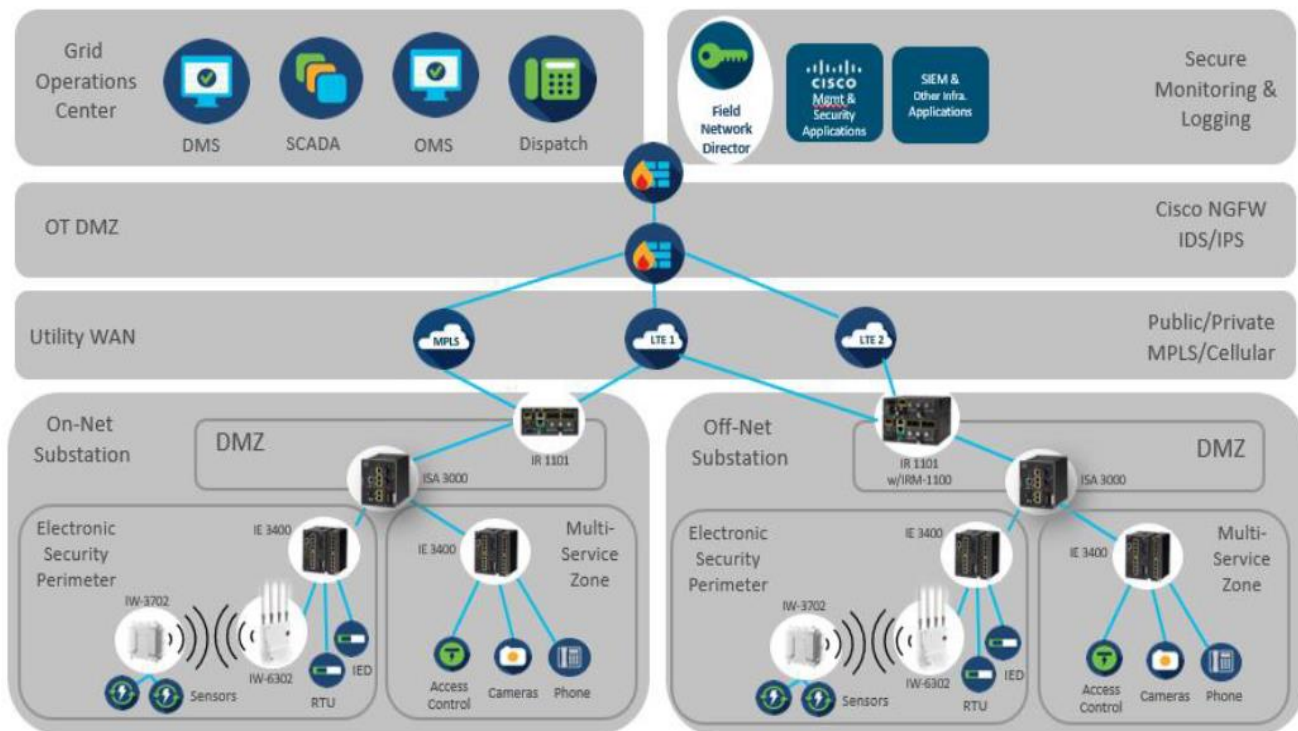
Part Number	Smart Account Mandatory	Description	Product Family / Service Level
Group Name: Cyber Vision			
CV-LICENSE	-	Cisco Cyber Vision Licenses	
SVS-CV	-	Embedded Support for Cisco Cyber Vision	
CBNB-E2SF-CV-ADV-P-5Y-10001-50000	-	SECURITY EA 2.0 CYBER VISION ADVANTAGE LICENSE	
CBNB-E2SF-CV-IDS-IC3000-P-5Y	-	CYBER VISION SENSOR IDS LICENSE FOR SECURITY CHOICE EA	
CBNB-E2SF-F-FPR1120T-P-5Y	-	SEC EA 2.0 CHOICE FPR1120 THREAT DEFENSE THREAT, MALWARE URL	
VMW-VSP-STD-5A=	-	VMware vSphere 7 Std (1 CPU, 32 Core) 5-yr, Support Required	
CON-ISV1-VSXSTD5A	-	VSphere Standard for 1 CPU; ANNUAL List 5-YR Req'd	
UCS-VMW-TERMS	-	Acceptance of Terms, Standalone VMW License for UCS Servers	
Group Name: Switch Sites POP			
IC3000-2C2F-K9	-	Industrial Compute appliance	
CON-SNT-IC30002C	-	SNTC-24X7X4 Industrial Compute aIndustrial Compute a	
SW-IC3000-U-K9	-	Cisco Software for IC3000 Industrial Compute Gateway	
CV-IC3000-APP	-	Cyber Vision Sensor for IC3000	
IOT-UTILITIES	-	Utilities Industry Solutions; For tracking only.	
IOT-SUBSTATION	-	Substation Automation; For tracking only.	
Group Name: Firewall			
ISA-3000-4C-FTD	-	ISA 3000 4 copper ports FTD Unified image	
CON-SNT-ISA3004D	-	SNTC-8X5XNBD ISA 3000 4 copper ports FTD Unified imag	
IOT-UTILITIES	-	Utilities Industry Solutions; For tracking only.	
IOT-SUBSTATION	-	Substation Automation; For tracking only.	
ISA-FTD6.6-K9	-	Cisco FTD unified software v6.6 for ISA3000	
L-ISA3000T-T=	-	ISA 3000 FirePOWER Threat Defense & Protection Smart License	
L-ISA3000T-T-5Y	-	ISA 3000 FirePOWER Threat Defense Smart License 5Y subs Start Date 19-Apr-2022	
SF-FMC-VMW-300-K9	-	Cisco Firepower Management Center, (VMWare) for 300 devices	
CON-ECMU-SFFMCVMW	-	SWSS UPGRADES Cisco Firepower Management Center, (VMWa	
Group Name: Switch Industrial Tipo I			
IE-3400-8T2S-E	-	Catalyst IE3400 with 8 GE Copper and 2 GE SFP, Modular, NE	
CON-SNT-IE340088	-	SNTC-8X5XNBD Catalyst IE3400 Rugg	
IOT-UTILITIES	-	Utilities Industry Solutions; For tracking only.	
IOT-SUBSTATION	-	Substation Automation; For tracking only.	
SD-IE-4GB=	-	IE 4GB SD Memory Card	
Group Name: Default			
STK-RACK-DINRAIL=	-	19" DINRAIL kit to replace STK-RACKMNT-2955=	

 <p>CPFL ENERGIA</p> <p>Público</p>	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

6.4. TOPOLOGIA ILUSTRATIVA DA SOLUÇÃO




Proposed Substation Architecture – Foundational Phase 1

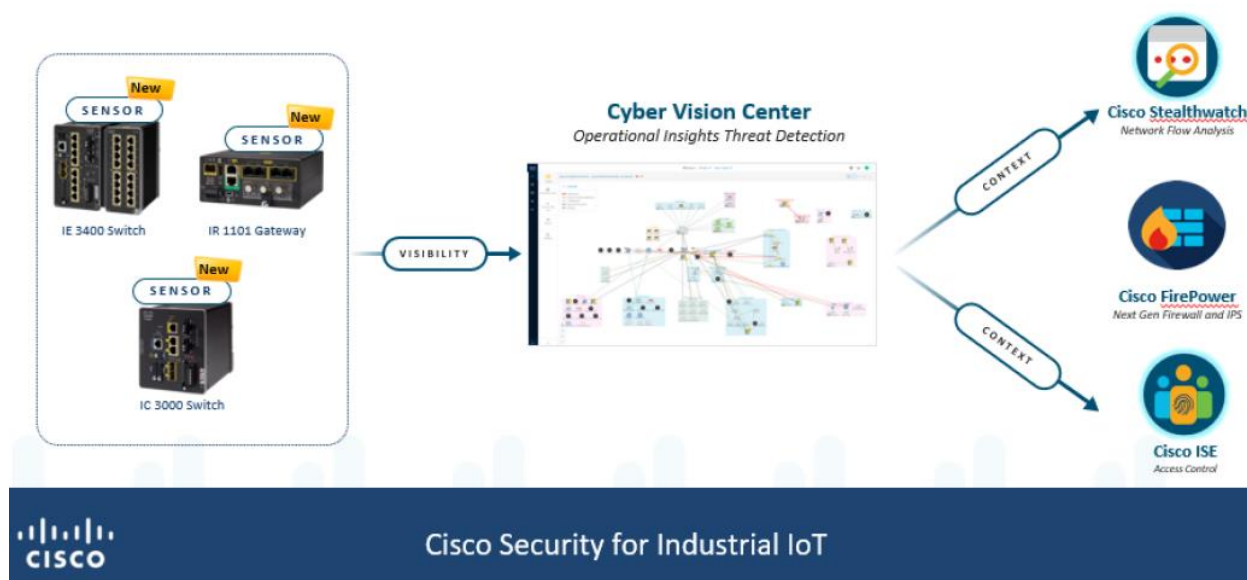


6.5. COMPONENTES DA SOLUÇÃO

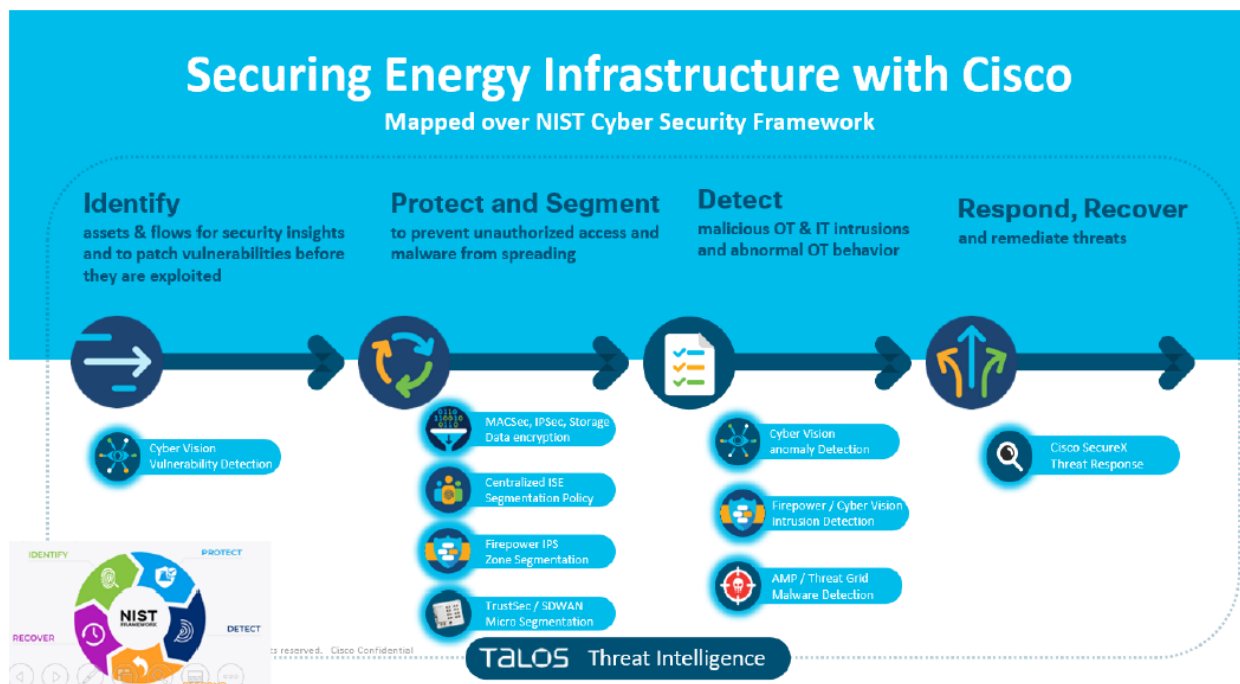
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	8 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

Comprehensive Industrial IoT Security Architecture




6.6. METODOLOGIA DE SEGURANÇA & CYBER VISION



CISCO Cyber Vision

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	9 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

O Cisco Cyber Vision permite que as organizações garantam a continuidade, resiliência e segurança de suas operações industriais, fornecendo visibilidade contínua de suas redes de controle industrial e gerenciando os riscos de ataques cibernéticos.

Visão geral do produto

A integração mais profunda entre TI, nuvem e redes industriais está expondo seus sistemas de controle industrial (ICS) a ameaças cibernéticas. À medida que você começa a capturar os benefícios de seus esforços de digitalização do setor e começa a implantar tecnologias de Internet das Coisas Industrial (IIoT), você precisa de uma solução de segurança cibernética para ajudá-lo a garantir a continuidade, resiliência e segurança de suas operações industriais.

O Cisco Cyber Vision foi projetado especificamente para que organizações industriais obtenham visibilidade total de suas redes industriais, para que possam detectar ameaças, garantir a integridade do processo, construir infraestruturas seguras, conduzir a conformidade regulatória e aplicar políticas de segurança para controlar riscos.

O Cisco Cyber Vision combina uma arquitetura exclusiva de monitoramento de borda e integração profunda com o portfólio de segurança líder da Cisco. Integrado ao seu equipamento de rede industrial da Cisco, ele pode ser facilmente implantado em escala para monitorar seus ativos industriais e seus fluxos de aplicativos em tempo real.

É a solução ideal para alimentar seu Centro de Operações de Segurança de TI (SOC) com contexto OT, para que você possa construir uma arquitetura unificada de segurança cibernética de TI/OT.

Firewall ISA 3000 Cisco

Desenvolvidos especificamente para suportar os ambientes industriais mais severos, esses firewalls industriais oferecem segurança de ponta a ponta intransigente com design e operação industriais em mente.

Visão geral do produto

O Cisco Secure Firewall ISA3000 é um verdadeiro firewall industrial que oferece proteção direcionada a OT com base em segurança comprovada de classe empresarial.

O ISA3000, com quatro links de dados, é um dispositivo robusto de montagem em trilho DIN que oferece a mais ampla variedade de controles de acesso, ameaças e aplicativos para os ambientes industriais mais severos e exigentes.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	10 de 17


 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL



Figura 1.

Cisco Secure Firewall ISA3000 com duas portas de cobre e duas de fibra (esquerda) ou quatro portas de cobre (direita)

O Cisco Secure Firewall ISA3000 oferece:

- Tráfego controlado de, para e entre células de manufatura ou zonas industriais;
- Conectividade WAN segura para subestações de energia e ativos industriais isolados
- Acesso remoto de classe empresarial flexível e seguro;
- Serviços críticos de infraestrutura de rede, como roteamento IP, NAT, DNS, DHCP e muito mais;
- Proteção inigualável contra ameaças para todos os níveis de rede e computação — desde switch, roteador, sistema operacional e infraestrutura de computação até sistemas de controle industrial;
- Amplo suporte para protocolos industriais para visibilidade e controle sobre todos os níveis de seus aplicativos no espaço industrial e empresarial;
- Mais níveis de segurança de continuidade de tráfego do que outras ofertas no espaço industrial;
- Critérios comuns para certificação de segurança de TI.

Switch IE 3400 Cisco


O Cisco Catalyst IE3400 Rugged Series inaugura a adoção generalizada de conectividade Gigabit Ethernet avançada em um switch modular de forma compacto desenvolvido especificamente para uma ampla variedade de aplicativos corporativos e industriais estendidos.

Visão geral do produto

Os switches Cisco Catalyst IE3400 Rugged Series oferecem conectividade Gigabit Ethernet avançada e de alta velocidade em um formato compacto e são projetados para uma ampla variedade de aplicações industriais onde são necessários produtos reforçados.

O design modular do Cisco Catalyst IE3400 Rugged Series oferece flexibilidade para expandir até 26 portas de Gigabit Ethernet com uma variedade de opções de módulos de expansão. A plataforma foi construída para resistir a ambientes agressivos em manufatura, energia, transporte, mineração, cidades inteligentes e petróleo e gás. A plataforma IE3400 também é ideal para implantações corporativas estendidas em espaços externos, armazéns e centros de distribuição.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	11 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

A série IE3400 executa o Cisco IOS XE, um sistema operacional de última geração com segurança e confiança integradas, com inicialização segura, assinatura de imagem e o módulo âncora Cisco Trust. O Cisco IOS XE também fornece configuração orientada por API com APIs abertas e modelos de dados.

O Cisco Catalyst IE3400 Rugged Series pode ser gerenciado com ferramentas de gerenciamento poderosas, como o Cisco DNA Center e o Industrial Network Director, e pode ser facilmente configurado com uma ferramenta GUI moderna, fácil de usar e totalmente redesenhada chamada WebUI. A plataforma também suporta Full Flexible NetFlow (FNF) para visibilidade em tempo real dos padrões de tráfego e análise de ameaças com o Cisco Stealthwatch.

A série IE3400 (com módulo de expansão) tem suporte de energia de até 480 W para PoE/PoE+, compartilhado em 24 portas, e é ideal para conectar dispositivos finais alimentados por PoE, como câmeras IP, telefones, pontos de acesso sem fio, sensores e muito mais.



Gateway IC 3000 Cisco


O Cisco IC3000 Industrial Compute Gateway transforma os negócios capturando dados de ativos legados e derivando business intelligence na borda da rede.

Visão geral do produto

O gateway de computação industrial Cisco IC3000 estende a inteligência de dados até a borda da rede da Internet das Coisas (IoT) para conectar perfeitamente a rede baseada em intenção e a malha de dados IoT em uma solução completa de ponta a ponta para aplicativos como estradas inteligentes, fábricas etc.

O gateway IC3000 é construído com o mesmo sucesso industrial que o design de hardware dos switches Cisco Industrial Ethernet 4000 Series, mas é dedicado a levar a inteligência ao limite. Ele tem duas portas Ethernet e duas portas de fibra Small Form-Factor Pluggable (SFP) em um dispositivo robusto montado em trilho DIN que oferece a mais ampla gama de aplicações para os ambientes industriais mais severos e exigentes.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	12 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL


O gateway IC3000 oferece o próximo nível de poder computacional, acima do IR 809 e IR 829, para aplicativos que exigem mais poder de processamento para análise de dados e tomada de decisões críticas em tempo real na borda da rede IoT. Ele permite aplicativos de estradas inteligentes, como detecção de padrões de tráfego, avisos de condições meteorológicas perigosas e detecção de condições da estrada.

Com interfaces integradas que suportam uma ampla variedade de padrões industriais e um kit de ferramentas de desenvolvimento simples, o IC3000 permite que os desenvolvedores de aplicativos liberem sua criatividade na criação de aplicativos que aproveitam a riqueza dos dados de IoT.

O gateway de computação industrial Cisco IC3000 é totalmente compatível com o Cisco IoT Field Network Director para implantação sem toque, gerenciamento do ciclo de vida, gerenciamento de aplicativos, monitoramento e solução de problemas com segurança em escala a partir de um único painel. Com seu suporte para o Cisco Kinetic™ Edge and Fog Processing Module, que calcula dados em nós distribuídos, ele se integra perfeitamente ao Cisco Kinetic Data Control Module, que move os dados certos de um conjunto diversificado de dispositivos para os aplicativos baseados em nuvem certos no momento certo, de acordo com a política definida pelo proprietário dos dados.



N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	13 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

Conversor 125VCC/48VDC Proteco

Desenvolvido pela Proteco, este modelo converte 125Vcc em 48Vcc/12A, utilizado para fixação em rack 19". Destinado a alimentar equipamentos que requerem funcionamento ininterrupto (Operações Críticas).



GERAL

Ventilação	NATURAL
MTBF	> 115.000 horas
Temperatura de operação	0 - 45°C
Umidade Relativa	15% a 95%
Rendimento	> 85%


ENTRADA

Tensão nominal de entrada	125Vcc
Faixa de variação	105Vcc até 147Vcc

SAÍDA

Tensão nominal de saída	48Vcc
Capacidade	12A
Regulação Estática de tensão	±1%
Regulação Dinâmica de Tensão	< 25ms
Ripple RMS	≤ 100mV
Ripple Psofométrico	< 2mV
Limitação de corrente de saída	ajustável entre 50% a 110%

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	14 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

Servidor

Os requisitos de segurança para servidor deve ser considerado o tamanho e a completude do projeto de novas instalações, pois dependendo será preciso revisitar a necessidade de upgrade no servidor ou aumento de recursos computacionais, para atender as necessidades técnicas e cibernéticas de cada subestações.

IMPLEMENTAÇÃO FABRICANTE (AS) – CISCO

Deve ser considerando serviço de implementação/configuração do fabricante para os produtos da proposta.

→ Desenho de Alto e Baixo Nível da solução de subestações contemplando:

- Solução de Cyber Vision com Centers + Global em DCs com sensores entre IC e IE.
- FWs ISA3k espalhados por subestações.

→ Implantação do CORE da solução do Cyber Vision.

→ A Cisco fará a implementação de POPs/Subestações, com elaboração de plano de implementação, testes de validação da solução e AS-BUILT

A princípio está sendo considerado os seguintes modelos de sites:

- Modelo 1 – POP de DC com ativação do sensor IC3k.
- Modelo 2 – Subestação com ISA3k + IE3400 com IDS.
- Modelo 3 – Subestação com IE3400 com IDS.

→ Suporte a Pós Implementação para sanar dúvidas e troubleshooting

→ Uma sessão de passagem de conhecimento para o projeto.

✓ **Características:**


- Overview da solução contratada;
- Desenho da solução
- Configuração dos Equipamentos
- Preparação do equipamento e configurações iniciais (pré-instalação);
- Tuning das configurações observando produção;
- Quality Assurance e recomendação de melhorias;

PREMISSAS DA IMPLEMENTAÇÃO

Premissas técnicas deverão estar sendo consideradas, sendo:

- Para sensoriamento das subestações, estamos considerando os dispositivos por subestação.
- Ativação da feature avançada de IPS está sendo considerado no serviço do ISA3k.
- Todo trabalho será acompanhado por um funcionário da CPFL Energia, sendo o mesmo a

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	15 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

interface com as demais áreas da empresa;

- Os equipamentos devem estar instalados no rack e energizados;
- Toda a migração dos equipamentos de produção (roteadores, switches, etc), caso seja necessário, será de responsabilidade do cliente e/ou da integradora responsável pelo projeto;
- Toda inclusão de novos equipamentos (roteadores, switches, etc), caso seja necessário, será de responsabilidade do cliente e/ou da integradora responsável pelo projeto;
- A sessão de passagem de conhecimento poderá ser feita de maneira virtual.

IMPLEMENTAÇÃO/CONFIGURAÇÃO/INSTALAÇÃO

Os serviços de implantação, envolvem a avaliação do ambiente atual, elaboração do projeto, instalação, configuração e documentação dos equipamentos e sistemas definidos no “Anexo 2 – Termo de Referência dos Equipamentos” em atendimento à “RFP – Solução de Infraestrutura – Subestações” da CPFL Energia.

É importante ressaltar que os serviços serão realizados em conjunto com o fabricante (Cisco), atendendo aos requisitos descritos na “ET-Infraestrutura Subestações -Serviço”.


ESCOPO DE SERVIÇO

- Realizar Assessment/Avaliação do ambiente atual em localidades selecionadas, para obtenção de informações necessárias para realização do projeto;
- Realizar overview da solução contratada para a CPFL Energia;
- Desenho de Alto e Baixo Nível da solução contratada;
- Realizar plano e escopo de trabalho para aprovação da CPFL Energia;
- Realizar a instalação física, configuração e ativação dos sistemas e equipamentos propostos;
- Realizar operação assistida durante ativação dos sistemas/equipamentos;
- Demais configurações lógicas, garantindo o pleno funcionamento de toda solução (Tunning e Quality Assurance);
- Documentação do projeto (As Built);
- Passagem de conhecimento da solução a equipe da CPFL Energia;
- Realizar suporte pós-implantação por 30 dias, após entrega formal do projeto.
- Fornecimento dos Patch Cords e instalação física dos equipamentos são responsabilidade da fornecedora.

7.CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
RFP	Sistema CRM Dynamics	Backup	Por número de contrato	Backup	Deletar

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	16 de 17

 Público	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Requisitos de Segurança Cibernética para Subestações de Distribuição da CPFL

8. ANEXOS



IE-3400.pdf



ISA-3000.pdf



Cisco Cyber Vision
Architecture Guide - 4

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Paulista	EIS	Mateus Augusto Pereira Rocha
Paulista	EIS	Leandro Barbosa do Carmo
RGE	EIS	Alexandre Mundim de Oliveira

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
-	-	Criação do documento

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
19474	Instrução	1.0	Emerson Cardoso	10/05/2023	17 de 17