una empresa ISA

Implementación de controles de ciberseguridad en centro control SCADA E.M.S

Rubén Dario Villa Trujillo
rvilla@xm.com.co
Octubre 2017

una empresa ISA

Contexto

2 Clasificación de activo

Gestión seguridad ciberactivos

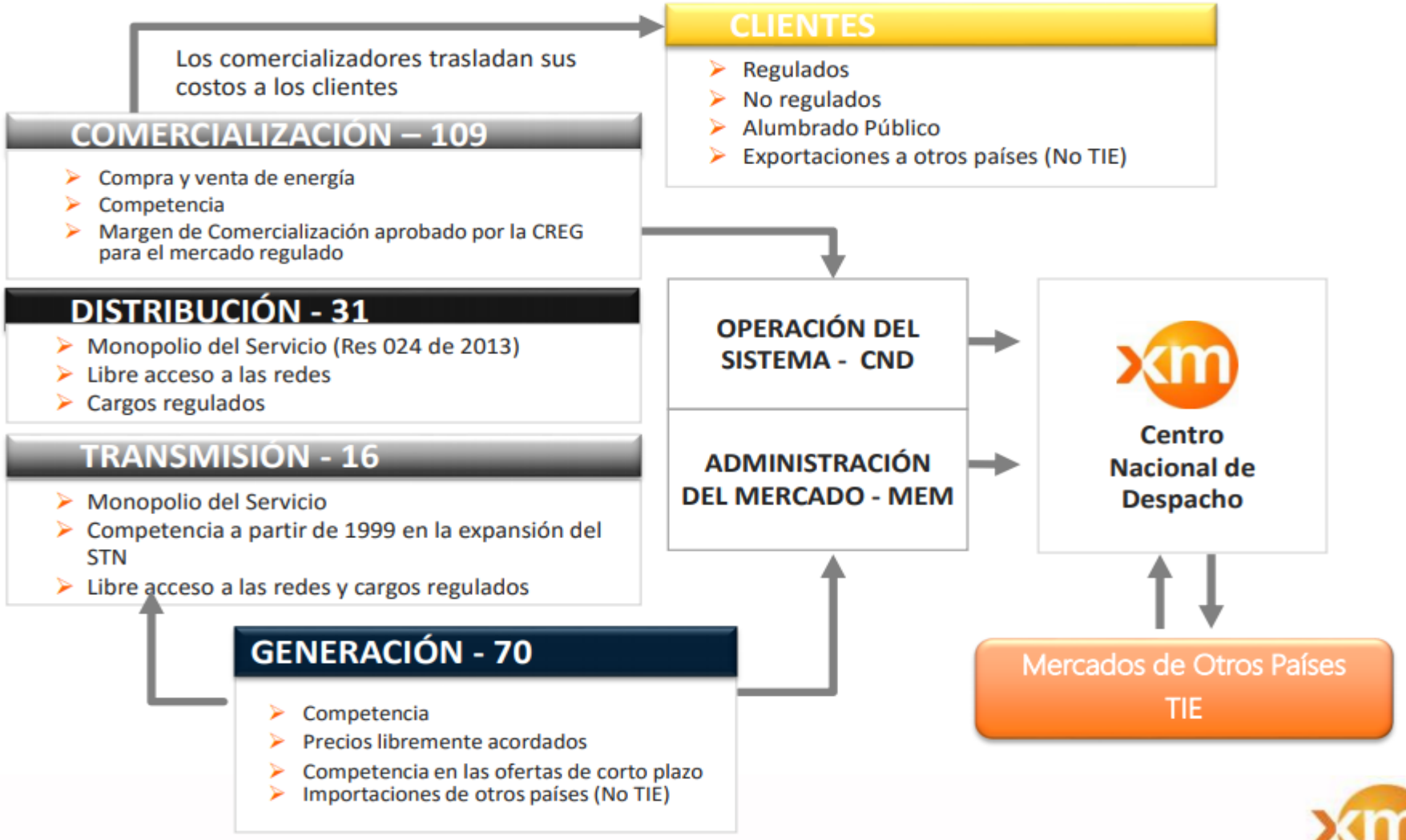
4 Seguridad Física

Plan de recuperación

Contexto

una empresa ISA

XM Operador del Sistema Eléctrico Colombiano



Número de agentes por actividad, Fecha del reporte: 16 de agosto de 2016, fuente: http://paratec.xm.com.co

Acuerdo 788 ciberseguridad

Generalidades

Inicio 2010 - Aprobado 3/9/2015

- ✓ Acuerdo de obligatorio cumplimiento
- ✓ Basada en el estándar Nerc Cip v4
- ✓ Generación, transmisión, distribución y operación

Contenido:

- ✓ Identificación de ciberactivos
- ✓ Gestión seguridad ciberactivos
- ✓ Seguridad Física ciberactivos
- ✓ Plan de recuperación

Acuerda

1. Aprobar la guía de ciberseguridad
2. Establecer responsable de ciberseguridad por compañía (3/04/2017)
3. El CNO definirá y estructurará un plan de trabajo que incluya actividades de sensibilización, comunicación, entrenamiento y socialización
4. Identificación activos críticos y ciber activos en 3/09/2016

Clasificación de activos

una empresa ISA

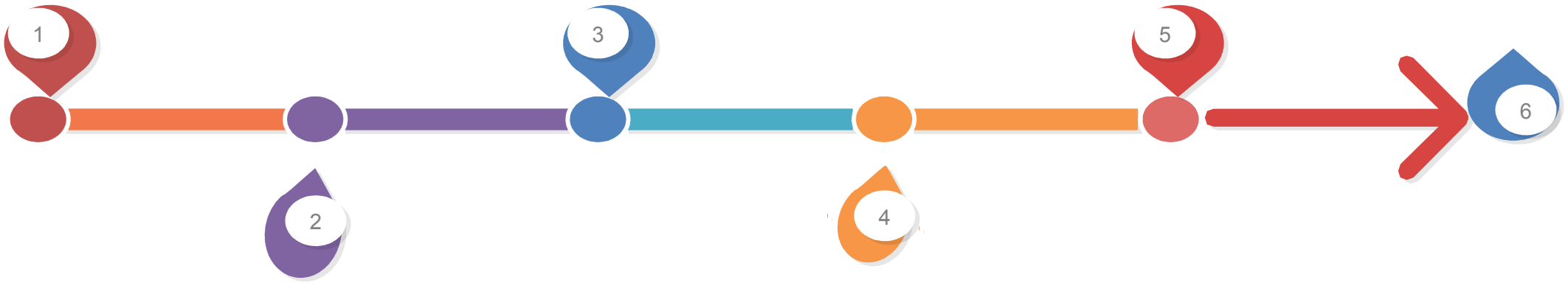
Clasificación de activos

Activos Críticos

Ciber activos críticos

Catalogo de activos.

Protección Nerc Cip



Ciber activos

Taxonomía

Se hace en cada compañía y luego XM centraliza la información , la entrega el grupo de Infraestructuras Criticas Nacionales del Ministerio de Defensa

Activos criticos

- Instalaciones de transmisión operadas a 220 KV o mayor, es decir, que pertenezcan al STN (Sistema de Transmisión Nacional).
- Instalaciones de transmisión operadas a 110 kV o más y que contengan más de una instalación con otros niveles de tensión.
- Instalaciones de transmisión que, a criterio del operador del sistema, pertenezcan a cortes críticos desde el punto de vista de confiabilidad.
- Instalaciones de transmisión operadas a 220 KV o mayor, es decir, que pertenezcan al STN (Sistema de Transmisión Nacional).
- Instalaciones de transmisión que conectan generación al sistema y que su indisponibilidad podría indisponer equipos de generación como los considerados en los ítems 1.1. y 1.3.
- Cada centro de control o centro de control de respaldo usado para ejecutar las obligaciones funcionales del operador del sistema, Generador, Transmisor o Distribuidor

Ciber activos y ciberactivos criticos

Ciberacticos

Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

Ciberacticos críticos

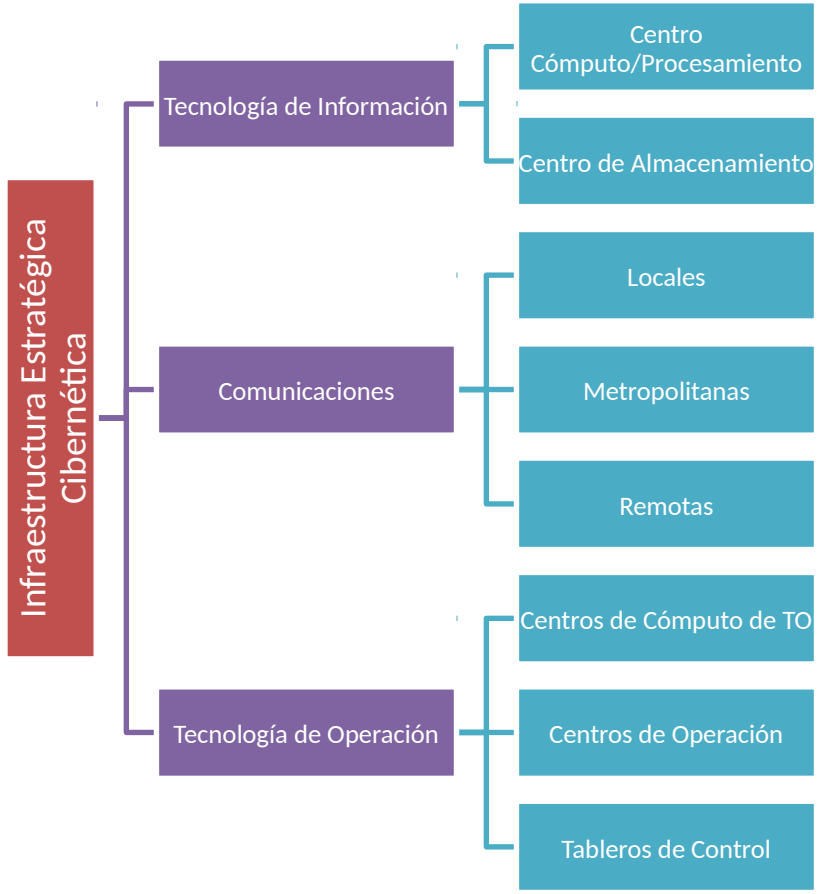
El ciberactivo usa un protocolo enrutable con un centro de control

El ciberactivo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica

El ciberactivo es accesible por marcación.

Identificación de ciber activos criticos

Taxonomía



Detalle de taxonomía

Centro de Computo de TO

- Servidores de proceso
- Sistemas de Intercambio de Información entre redes TO/TI
- Sistemas de Sincronización de Tiempo

Centros de Operación

- Estaciones de operación
- Estaciones de ingenieria

Tableros de Control

- RTU
- IHM
- PLC

Ejemplo de Clasificación

Compañía	Activo critico	Ciber activo	Ciberactivo critico	Tipo
XM	Centro operación Principal			
XM	Centro operación respaldo			
XM	Centro operación Principal	SCADA EMS		Sistemas de Sincronización de Tiempo
XM	Centro operación respaldo	SCADA EMS		Servidores de proceso
XM	Centro operación Principal	SCADA EMS	firewall	equipo proteccion perimetro
XM	Centro operación respaldo	SCADA EMS	servidor RTC	equipo recibe señales ICCP

Gestión seguridad ciberactivos

una empresa ISA

Controles – definición de Perímetro

Centro de Control XM

TCP/IP

Sistemas Regionales de Control (SRCs)

IEC60870-6 [ICCP]

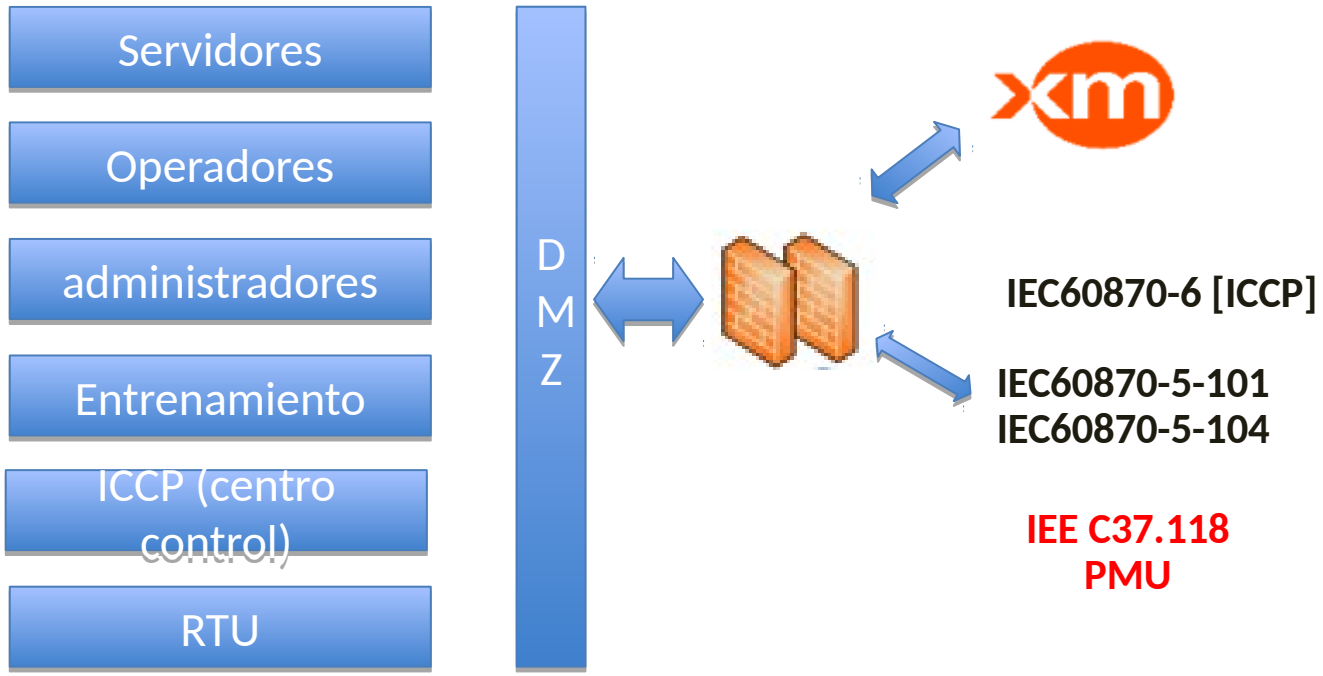
IEC60870-5-101
IEC60870-5-104

Subestaciones

Plantas Térmicas

Plantas Hidráulicas

Controles – definición de Perímetro



Controles Nerc Cip

- ✓ Definición perímetro lógico
- ✓ Separación de redes
- ✓ Acceso solo por DMZ
- ✓ Cero conexiones directas
- ✓ Control de acceso a la información
- ✓ Modelo de intercambio de información
- ✓ Identificación de protocolos
- ✓ Modelos de comunicación entre segmentos
- ✓ Convenio de cooperación Comando Conjunto cibernético colombia

Seguridad en Centro Control SCADA

General

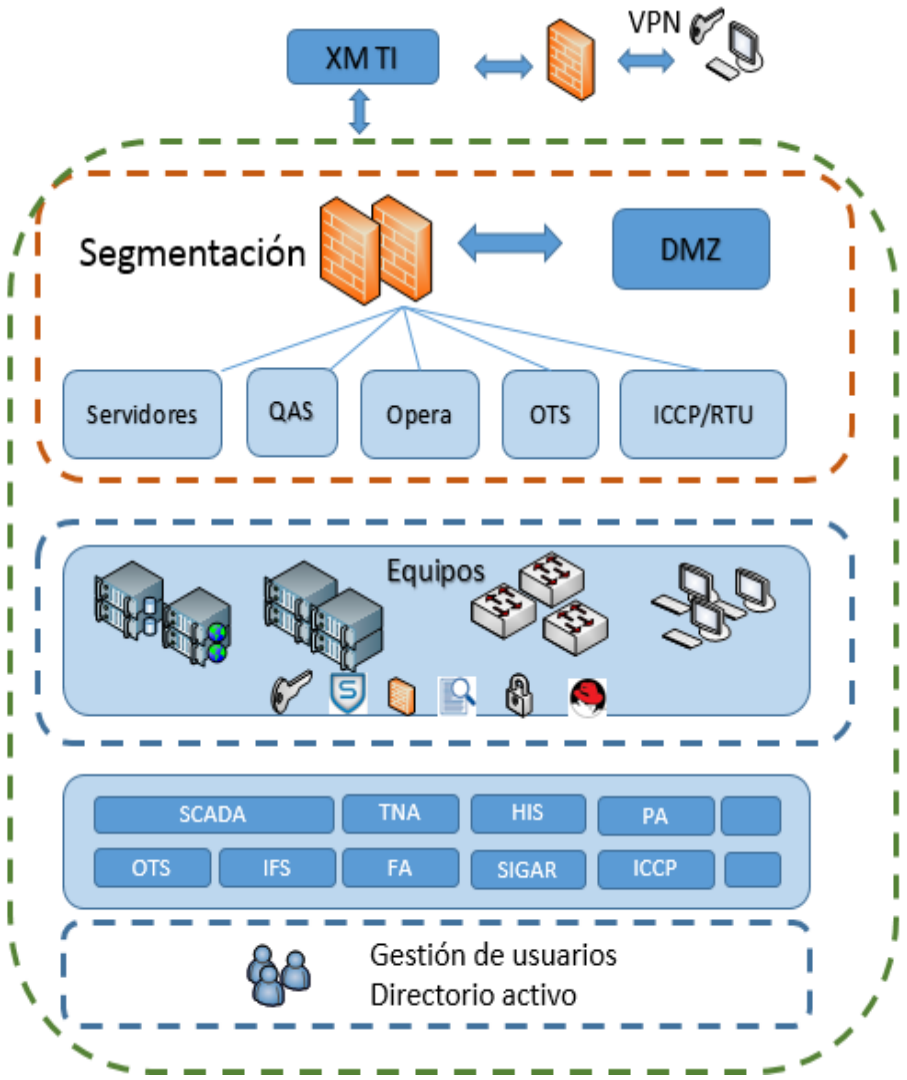
- ✓ Gestión de log y disponibilidad
- ✓ Gestión Configuración y cambios
- ✓ Análisis vulnerabilidades y pruebas de intrusión
- ✓ Backup

Equipos

- ✓ Cifrado comunicaciones
- ✓ Antivirus (Linux y Windows)
- ✓ Firewall de Windows e Iptables
- ✓ FAM (file alteration monitor)
- ✓ Hardening Puertos y servicio

Usuarios

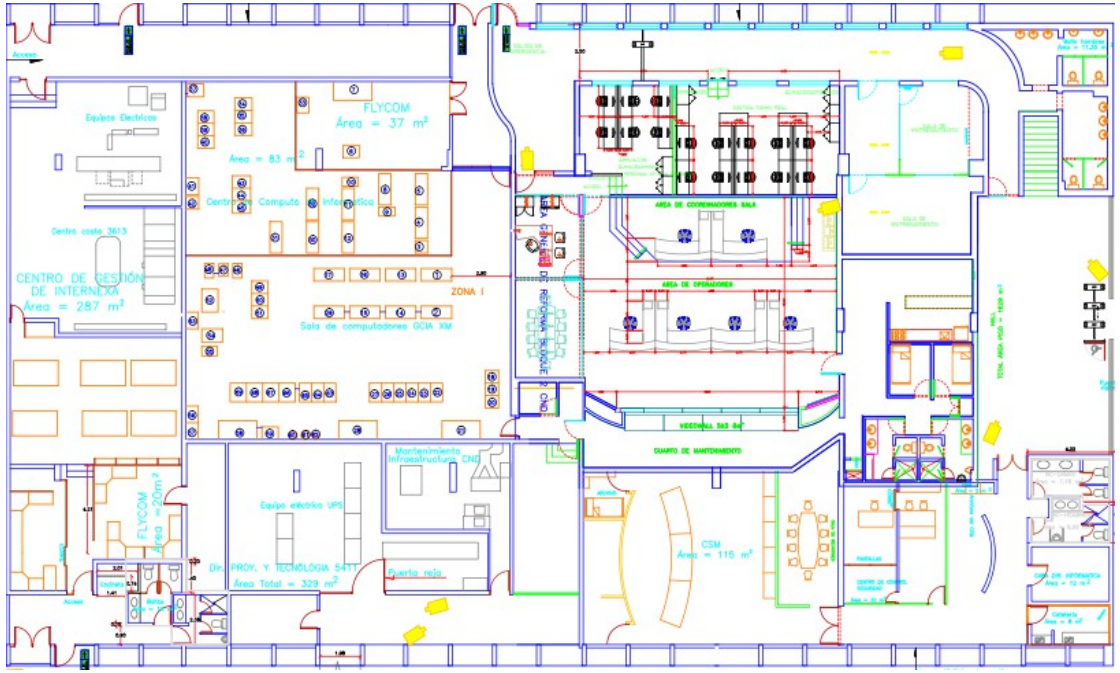
- ✓ Gestión de usuarios
- ✓ Directorio activo
- ✓ Segregación de funciones



Seguridad Física

una empresa ISA

Seguridad Física

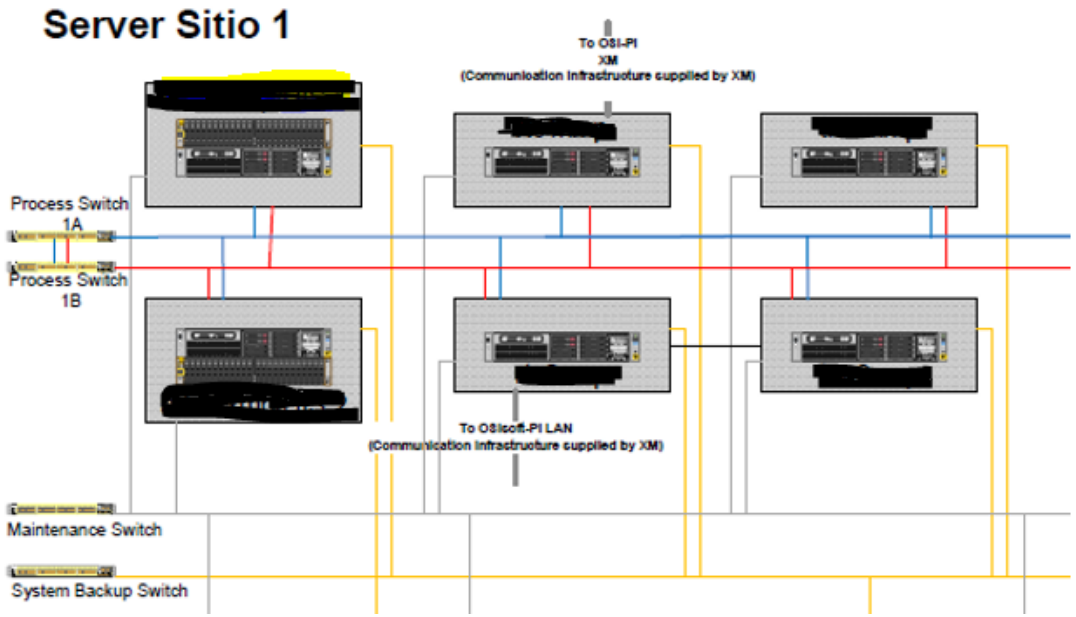


Controles Nerc Cip

- ✓ Ajustes en CCTV cámaras y grabación
- ✓ Ajustes en el control de Acceso: sensores de tarjetas, molinetes de acceso
- ✓ Restricciones de uso de móviles
- ✓ Botones de emergencia y pánico
- ✓ Potenciamiento de software de monitoreo
- ✓ Mantenimiento y pruebas equipos seguridad física

Plan de recuperación

una empresa ISA



Controles Nerc Cip

- ✓ Esquema de alta disponibilidad
- ✓ BIA
- ✓ Pruebas de continuidad procesos y conmutación
- ✓ Esquema de backups y recuperación
- ✓ Redundancias
- ✓ Multisitio (en proceso)

PREGUNTAS

una empresa ISA

Calle 12 sur 18 - 168 Bloque 2
PBX (57 4) 317 2244 - FAX (57 4) 317 0989
@XM_filial_ISA
Medellín - Colombia

una empresa ISA