Institución Universitaria

Modelo de ciberseguridad en las Unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico Nacional

Rubén Darío Villa Trujillo

Instituto Tecnológico Metropolitano

Facultad

Ciudad, Colombia

2019

Modelo de ciberseguridad en las Unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico Nacional

Rubén Darío Villa Trujillo

Tesis o trabajo de investigación presentada(o) como requisito para optar al título de:
Magister en Seguridad Informática

Director:
Magister Héctor Fernando Vargas Montoya

Línea de Investigación:
Seguridad de la información
Grupo de Investigación:
Automática, electrónica y ciencias computacionales

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2019

(Dedicatoria o lema)

A mi esposa y a mi hija, a mi madre y a mi hermano, a todos aquellos que hoy no están con nosotros, pero nos acompaña su recuerdo, a mis compañeros de trabajo y a todas aquellas personas que de una u otra manera han creído en mí y me dan su fuerza para culminar este logro profesional y una etapa más de mi vida

Agradecimientos

A mi familia y seres amados que siempre me apoyado en toda mi vida

Al Magister Héctor Fernando Vargas Montoya, quien como director de esta tesis de Maestría aporto sus conocimientos y experiencia en seguridad informática y metodología al servicio de este trabajo

A los docentes de la Maestría en Seguridad Informática del ITM, por la experiencia y conocimientos transmitidos, así como por su compromiso y esfuerzo en formar magister de calidad

A la Institución Universitaria ITM, por brindarme la posibilidad de formarme como profesional y poder optar por el título de Magister en seguridad informática

A la compañía XM S.A.ESP por permitirme participar en el proyecto del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico Nacional desde el punto de vista de seguridad y brindarme las herramientas necesarias para el desarrollo de tan importante proyecto

Resumen

El mapa de implementación del proyecto Sistema Inteligente de Supervisión y Control Avanzado (ISAAC) desarrollado por la compañía XM SA ESP, está basado en dispositivos PMU (Unidades de medición fasorial) los cuales hacen parte de la infraestructura eléctrica colombiana, éstos, son la base para el control de la frecuencia, sirven para dar respuesta efectiva de la oferta y demanda de energía.

Éste proyecto ha definido un modelo de ciberseguridad del proyecto ISAAC, para lo cual, se estableció (i) Una estimación de los riesgos asociados a ciberataques sobre dispositivos de supervisión PMU, (II) se definió un modelo para la implementación de controles, que reduzcan los niveles de riesgos sobre los dispositivos de supervisión PMU y (III) se implementó un ambiente de prueba que permita valorar los resultados del modelo propuesto y el impacto de los controles de seguridad sobre las funcionalidades de los equipos. Este proyecto no contempla la implementación de elementos de seguridad en su diseño ni controles complementarios sobre las PMU,

Los ciberataques cada vez más complejos y elaborados (ataques de hombre en el medio, alteración de datos, ataques de denegación de servicios distribuidos, suplantación, inserción de código, botnet, entre otros), el surgimiento de grupos especializados en construir software malicioso (malware, troyanos, APTS -amenazas persistentes en el tiempo, secuestro de información), el ciberespionaje y la situación compleja de nuestro país hacen que sea necesario la implementación de controles y modelos de ciberseguridad para proteger la infraestructura que soporta el sistema eléctrico

Dado lo anterior en éste trabajo de maestría, se diseñó un modelo de ciberseguridad para los elementos PMU en el proyecto ISAAC asociado al sistema eléctrico colombiano, que permite realizar una operación confiable y segura, mitigando con ello riesgos y mejorando la resiliencia ante posibles eventos de ciberseguridad sobre dichas PMU.

Palabras clave: Unidades de Medición fasorial (PMU), ciberseguridad, gestión del riesgo, Sistema Inteligente de Supervisión y Control Avanzado proyecto ISAAC, Sistema Interconectado Nacional (SIN)

Abstract

The implementation map of the Intelligent Advanced Monitoring and Control System (ISAAC) project developed by the company XM SA ESP, is based on PMU devices (Fasorial measurement units) which are part of the Colombian electrical infrastructure, these are the basis for frequency control, they serve to effectively respond to the supply and demand of energy.

This project has defined a cybersecurity model of the ISAAC project, for which, it was established (i) An estimate of the risks associated with cyber attacks on PMU monitoring devices, (II) a model for the implementation of controls was defined, which reduce the risk levels on the PMU monitoring devices and (III) a test environment was implemented to assess the results of the proposed model and the impact of safety controls on the functionalities of the equipment. This project does not include the implementation of security elements in its design or complementary controls on PMUs,

The increasingly complex and elaborate cyberattacks (man-in-the-middle attacks, data alteration, attacks on denial of distributed services, impersonation, code insertion, botnet, among others), the emergence of groups specialized in building malicious software (malware , Trojans, APTS - persistent threats over time, kidnapping of information), cyber espionage and the complex situation of our country make it necessary to implement controls and cybersecurity models to protect the infrastructure that supports the electrical system

Given the above in this master's work, a cybersecurity model was designed for the PMU elements in the ISAAC project associated with the Colombian electricity system, which allows a reliable and safe operation, thereby mitigating risks and improving resilience to possible events cybersecurity about these PMUs

Keywords: Fasorial Measurement Units (PMU), cybersecurity, risk management Sistema Inteligente de Supervisión y Control Avanzado proyecto ISAAC, Sistema Interconectado Nacional (SIN)

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de abreviaturas

Abreviatura	Termino
PMU	Unidades de Medición fasorial
ISAAC	Sistema Inteligente de Supervisión y Control Avanzado proyecto
SIN	Sistema Interconectado Nacional
SCADA	Sistema de Control Supervisión y Adquisición de Datos
EMS	Energy management system
WAMS	Wide Area Measurement System
ACIS	Asociación de ingenieros de sistemas
RTU	Unidad Remota de Transmisión
GPS	Sistema de Posicionamiento global
ISO	Organización internacional de normalización -
SGSI	Sistema de Gestión de seguridad de la información
FERC	Federal Energy Regulation Commission
BES Cyber	Bulk Electric System cyber
WAMPAC	Wide Area Monitoring Protection and Control
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
NERC CIP	North American Electric Reliability Corp. Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NCF	Nist Cybersecurity Framework
APT	Amenazas Persistente en el Tiempo
CCOCII	Comando Conjunto Cibernético
COLCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
SOC	Centro operaciones seguridad

1. Introducción

Las infraestructuras críticas[1] están definidas por el Consejo de la Unión Europea como: "*el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones* ", cuando éstas tienen una afectación, pueden repercutir gravemente en los estados. Las infraestructuras críticas constituyen estrategias capaces de mantener el desarrollo económico, culturar y progresista de un región o país.

En ese sentido, el planteamiento del proyecto de investigación Sistema Inteligente de Supervisión y Control Avanzado (ISAAC), desarrollado por XM S.A. E.S.P [2], consiste en diseñar la arquitectura y el ecosistema funcional para futuros sistemas de supervisión y control en tiempo real, como una evolución radical de los sistemas SCADA/EMS, constituyéndose en una de las infraestructuras críticas a nivel país. En el proceso se desarrollan elementos y tecnologías tales como el uso intensivo de equipos para medición fasorial (PMU), concentradores (PDC), Gateway/IDD, la implementación de tecnologías tipo Wide Área Measurement System (WAMS), funcionalidades distribuidas en subestaciones, comunicaciones IP, protección colaborativa y control distribuido [3].

El proyecto ISAAC proveerá un nuevo modelo de supervisión basado en comunicaciones IP, por lo que debe contar con un alto componente de seguridad informática y ciberseguridad, debido a que la infraestructura eléctrica es o puede ser blanco de ataques nacionales y/o internacionales.

Para la asociación de ingenieros de sistemas -ACIS [4] en su evaluación anual de posibles riesgos (encuesta 2018-2019) que se ocasionan en el uso de las TIC en temas de seguridad, se encuentra que el 55% corresponde a riesgos de ciberseguridad y el 43% son riesgos a la operación, lo que implica la necesidad de establecer controles que ayuden a reducir los respectivos riesgos de exposición, a través de diferentes estrategias organizacionales. En consecuencia, cada uno de los elementos de ISAAC, se encuentran propensos a ataques informáticos asociados con el ciberterrorismo que, en caso de ser exitosos, ponen en riesgo el Sistema Eléctrico Colombiano.

El problema detectado es que hasta el momento son equipos industriales o prototipos diseñados para cumplir funciones de supervisión y control, que no cuentan con un modelo de protección informática o ante ciberataques. Estos equipos se instalan en las redes de operación de los distintos agentes del mercado, con una distribución geográfica dispersa en el territorio nacional colombiano. Entre sus funciones se encuentran entregar información a los distintos agentes y alimentar los datos del operador del sistema eléctrico, quienes son los únicos autorizados para tener acceso a su administración y configuración.

El desarrollo de este proyecto de grado de maestría contempla el cumplimiento de los siguientes objetivos:

General:

Diseñar un modelo de ciberseguridad de las Unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (Isaac) para sistema eléctrico Nacional, con el fin de reducir los niveles de exposición a ataques informáticos.

Objetivos específicos

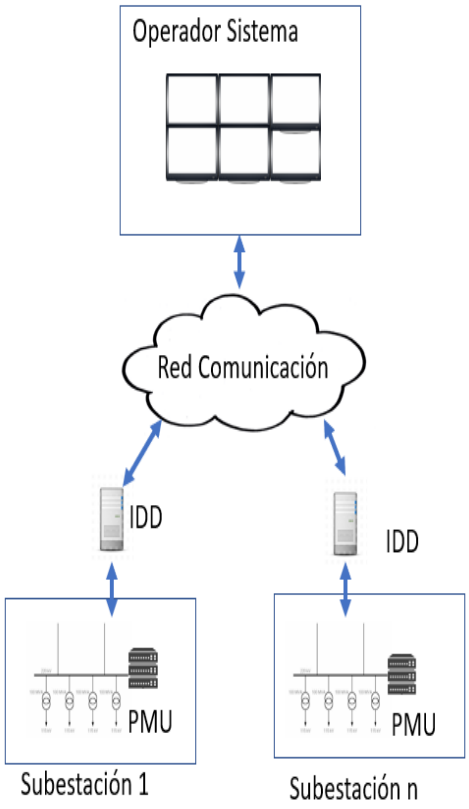
1. Establecer los posibles ataques y vulnerabilidades sobre dispositivos de supervisión PMU, con el fin de estimar los riesgos asociados a ciberataques sobre dispositivos de supervisión PMU.
2. Definir el plan de tratamiento de riesgos basados en los riesgos encontrados, que reduzcan los niveles de impacto sobre los dispositivos de supervisión PMU.
3. Valorar la implementación del plan de tratamiento de riesgos a través de la implementación de un ambiente de prueba controlado, que permita obtener los resultados del modelo propuesto y el imparto de los controles de seguridad sobre las funcionalidades de los equipos.

Este documento presenta de manera secuencial el cumplimiento de los objetivos, iniciando por un marco teórico y un estado del arte, luego se hace una descripción de la metodología usada para el cumplimiento de los objetivos y la documentación de los resultados, por último, se entregan las conclusiones, recomendaciones y trabajo futuro.

2. Marco Teórico y Estado del Arte

2.1 Marco Teórico

La supervisión y Control del sistema eléctrico colombiano actual está basado en tecnologías tipo SCADA/EMS con modelos definidos en los años 70s [5], a fecha de hoy ya se cuenta con gran cantidad de avances tecnológicos como lo son: la mejora en la comunicaciones, la evolución y surgimiento de nuevos protocolos, la nube, la analítica de datos, el bigdata y la necesidad de poder detectar y prever eventos como el apagón nacional en julio de 2007 Surge el proyecto sistema inteligente de supervisión y control avanzado (ISAAC), por sus siglas en inglés: Intelligent Supervisión and Advanced Control System) para el Sistema Interconectado Nacional.



En la figura 1 se presenta el esquema de alto nivel donde se observan los distintos elementos tecnológicos para lograr la supervisión en el Proyecto ISAAC:

- El centro de control, que está a cargo del operador del sistema, es el encargado de centralizar la información para la coordinación de la operación de Sistema Eléctrico Colombiano.
- Una red de comunicaciones por donde la información viaja basada en protocolos IP y el estándar IEEE C37.118 /61850 [6], utilizando servicios Tipo SOA y CIM
- Los dispositivos Gateway IDD ubicados en sitios como subestaciones de los distintos agentes del mercado que serán los encargados de centralizar los datos que emiten las PMU, realizar la inteligencia y toma de daciones automáticas para el sistema.
- Las PMU son los dispositivos finales de la cadena, son las encargadas de realizar la medición fasorial y enviar hasta 80 señales por segundo al centro de control para su supervisión, estas están instaladas en terminales/bahías de las distintas subestaciones del sistema Interconectado Nacional. [5]

Figura 1 Estructura de supervisión del proyecto ISAAC. Fuente propia

Como lo indican los autores de [5], investigadores principales de XM encargados de desarrollar el nuevo modelo de supervisión, el proyecto SIRENA tiene como objetivo diseñar la arquitectura, las características funcionales y un prototipo para los futuros sistemas de supervisión y control en tiempo real para un periodo de tiempo comprendido entre 2011 y 2025, los cuales se deben apalancar en la evolución de los siguientes temas:

- Integración de la Medición Fasorial en la supervisión
- Desarrollo de funcionalidad de supervisión y control distribuida en subestaciones
- Infraestructura de Comunicaciones (Redes IP y SOA)
- Desarrollo de Protección Colaborativa
- Desarrollo de programa Conciencia Situacional

Las PMU son sistemas de medición que actualmente se están instalando a nivel mundial, La fase (el ángulo) de fasores de tensión medidos por las unidades de gestión ayudan directamente en el cálculo de los flujos de potencia real en la red, y por tanto, pueden ayudar en la toma de decisiones en el centro de control en el balance oferta/demanda, Debido a que muestran detalles en la supervisión (hasta 80 señales por segundo) que los mecanismos actuales que son las RTU no se pueden evidenciar.

Las PMU utilizan el sistema de posicionamiento global (GPS) para dar a las mediciones fasorial precisión de fecha y hora. Por lo tanto, esta mide la diferencia de fase entre las tensiones en los extremos de una línea de transmisión, en un instante dado, este dato es importante para conservar los niveles de tensión y la frecuencia del sistema eléctrico. Los concentradores de datos de fasores combinan los datos de múltiples unidades de gestión y proporcionan datos alineados en el tiempo establecido para una región en particular al control centrar, como lo indica [7]

Actualmente no se cuentan con reportes públicos de incidentes sobre unidades de medición fasorial (PMU) en producción, dado su carácter de confidencialidad y de posibles impactos a la seguridad nacional, con posibles incidencias a nivel mundial, sin embargo, el modelo de respuesta a incidentes en Colombia para el sector eléctrico se apalanca en el Documento Conpes 3854[8] política de seguridad digital, en el cual especifica los modelos de identificación y clasificación de las infraestructuras críticas colombianas, actualmente está en proceso de definición el Plan Sectorial de Protección y Defensa para el Sector Electricidad en Colombia por parte del grupo de trabajo de infraestructuras críticas Colombianas adscrito al ministerio de defensa [9] y que esta trabajando de manera paralela con el consejo Nacional de Operación (CNO)[10]para la definición e implementación de mecanismos que permitan reportar, identificar y contener incidentes sobre infraestructura del sector incluyendo las PMU.

XM sustenta su política de riesgo en las normas ISO 31000 y la ISO 27005, la cual se basa en escenario de riesgo donde ya se tiene contemplado el escenario de ciberataque, por tal motivo se utilizaran estos referentes, asi mismo, es necesario conocer el los ciclos de vida de un ataque, y para la definición de controles y el modelo se utilizaran los estándares Nerc cip v6 [11] (The North American Electric Reliability Corporation Critical Infrastructure Protection estándar de seguridad del sistema eléctrico Norteamericano, sobre el cual se basa el acuerdo 1241[12] del consejo nacional de operación y el Framework for Improving Critical Infrastructure Cybersecurity de NIST [13] estándar relacionado con la seguridad de infraestructuras críticas Nortemaricanas .

2.1.1 Proceso de gestión de riesgos

Así mismo, La organización internacional de normalización - ISO ha generado una serie de normas concernientes a la gestión de riesgos, en la que se resalta la ISO 27005:2018 (Information technology Security techniques Information security risk management) enfocada a la seguridad de la información, dicha norma proporciona directrices que ayudan a la preservación de la seguridad de la información, elaborada y actualizada por la misma organización[14]. Dicha norma establece dentro de su proceso de gestión de riesgos los siguientes pasos:

1. **Establecer el contexto**: En esta etapa se define el contexto al cual se le hará un análisis de riesgos y dentro del contexto, es posible la definición de un alcance como tal.
2. **Identificación de riesgos**: Acá se hace un levantamiento de activos de información que hacen parte del contexto, para luego obtener un listado de amenazas y vulnerabilidades.
3. **Análisis de riesgos**: En esta etapa se hace un cruce de escenarios sobre la aplicabilidad de las amenazas vs. los activos de información con base en sus vulnerabilidades.
4. **Evaluación de riesgos**: Se definen las tablas de probabilidad e impacto (factor de impacto, que puede ser a la información, operación, imagen, económico, entre otras). Luego se hace una calificación de los escenarios de riesgos y se obtiene el mapa de aceptabilidad.
5. **Tratamiento de riesgos**: En consideración con los riesgos altos, se hace un plan de tratamiento de riesgos, consistente en definir si éstos de transfieren, aceptan, controlan o se evitan.
6. **Comunicación y consulta**: En un subproceso que indica que las partes interesadas deben estar enteradas del proceso.
7. **Monitoreo y revisión**: Se debe establecer un plan de monitoreo de los riesgos y realizar las revisiones de manera periódica.

El entender los procesos de gestión de riesgo ayuda al desarrollo del trabajo, debido a que este análisis es fundamental para poder definir el estado actual del proyecto, la definición de planes de acción y la evolución después de implementar controles con el fin evidenciar la efectividad del modelo de ciberseguridad.

Definiciones de seguridad

Para comprender el proceso de gestión de riesgos, es necesario la definición de los siguientes conceptos los cuales fueron tomados de la norma ISO 27000:2013[16] y se utilizan en el desarrollo del proyecto :

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del sistema de gestión de seguridad de la información (SGSI), que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.
- Consecuencia: Resultado de un evento que afectan a los objetivos
- Control: Medida que puede modificar un riesgo.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

2.1.2 Ciclo de vida de un ataque dirigido

El ciclo de vida de una ataque fue definido en Cyber-Kill Chain [15] que fue publicado como parte del modelo de para la identificación y prevención de la actividad de intrusiones cibernéticas.

En el modelo se especifican 7 fases o pasos que una atacante debe contemplar para alcanzar un objetivo., ver figura 2 Estos pasos son:

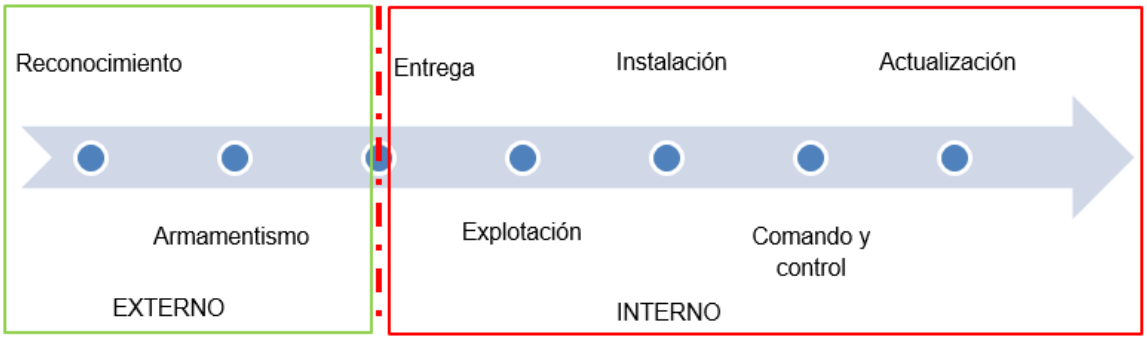


Figura 2: Ciclo de vida de un ataque o Cyber-Kill Chain. Fuente propia a partir de [14]

1. **Reconocimiento Externo**: Esta es la etapa de exploración, en ella se explora toda la información pública o expuesta de la compañía como los son: información tecnológica, redes sociales, correo, publicaciones, sitios web entre otros.
2. **Armamentismo y Paquetización**: El atacante realiza exploraciones en busca de fallas de seguridad, vulnerabilidades u omisiones, identificado o desarrollando las herramientas que puede utilizar para el poder lanzar el ataque.
3. **Entrega:** Es una de las etapas más críticas de la cadena debido a que atacante propicia que el usuario final o las tecnologías reciban el medio por el cual el cual puede ingresar a la plataforma o información, por ejemplo: entrega de un malware o programa dañino, robo de credenciales, explotación de una vulnerabilidad entre otros. En esta etapa se define si el atacante logró infiltrar la organización o si por el contrario permanece afuera de esta.
4. **Explotación**: Después de ser entregado el atacante ya se encuentra en la red, ya se explotó la debilidad que presenta la red, comienza a buscar modelos de propagación o de escalamiento de privilegios de manera sigilosa para no ser detectado y lograr su objetivo final.
5. **Instalación**: El atacante ya está dentro de su objetivo, ya lo que debe es buscar la forma de comunicarse con el exterior para poder sacar la información o lograr acceso remoto sin ser detectado.
6. **Comando y Control**: En esta fase, el adversario ya tiene el control absoluto de alguna tecnología o plataforma, comienza a utilizar instrucciones de comando y control para lograr el objetivo trazado
7. **Actuación en el Objetivo**: En esta fase final, el adversario roba los datos y/o daña los activos (ficheros, equipamiento) mientras permanece tiempo en la organización para identificar más

objetivos, expandirse dentro de ella y -lo más crítico de todo- seguir exfiltrando datos. La cadena se repite iterativamente.

Es importante aprender a conocer cada uno de estos elementos y como monitorearlos, poder identificar el nivel o estado en que se encuentra un ataque y cuáles serán sus próximos pasos, estos elementos son fundamentales para comprender que puede pasarle a la red de investigación de las PMU, la cual se puede ver seriamente afectada si se presenta una intrusión de un atacante que logra hacer comando y control estas, posterior altera las medidas o genera afectación de estas, lo cual afecta las capacidades de supervisión del sistema eléctrico y puede llevar a una toma errada de decisiones por parte de los operadores del sistemas que puedan causar una demanda no atendida o un apagón.

2.1.3 Normatividad y estándares

Se describe a continuación las normas y estándares que se deben contemplar apara desarrollar modelo se ciberseguridad de las PMU, esta contempla estándares de seguridad de la información: la ISO 27001:2013, estándares de seguridad para infraestructuras criticas como el Nist Cibersecurity Framewor y estándares específicos para el sector eléctrico norteamericano como el Nerc Cip en sus versiones más recientes.

- **Normatividad ISO 27001:2013**

La norma ISO 27001 [16] es una norma generada por la Organización Internacional de Normalización (ISO) que está basada en la norma británica BS 7799-2, se enfoca en cómo hacer la gestión del Sistema de Gestión de seguridad de la información (SGSI), su primera versión surgió en 2005 y actualmente se encuentra en la versión 2013 y se conoce como ISO/IEC 27001:2013.

La norma basa su implementación el ciclo PHVA y establece las siguientes etapas:

- **Etapa de Planificación: Establecer el SGSI**

En esta etapa se debe definir y Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.

- **Etapa de ejecución (Hacer): Implementar y operar el SGSI:**

En esta etapa se debe implementar y operar la política, los controles, los procesos y los procedimientos del SGSI

- **Etapa de Verificación: hacer seguimiento y revisar el SGSI**

En esta etapa se debe evaluar y medir el desempeño del proceso basado en la política y los objetivos de seguridad y la experiencia práctica, reportar los resultados a la dirección

- **Etapa de Actuación: Mantenimiento y mejora continua del SGSI**

En esta etapa se debe emprender acciones correctivas y preventivas basados en los resultados de la auditoría interna del SGSI y la revisión por la dirección.

Adicionalmente la norma cuenta con un Anexo técnico que contiene 114 controles que se deben implementar, y se encuentran separados en los siguientes dominios:

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía -Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.
- Cumplimiento: A.18.

Esta normatividad es importante para este trabajo debido que la compañía XM está certificada en la norma ISO 27001:2013 en todos sus procesos, y este proyecto de investigación debe cumplir los controles para su posterior entrada a producción.

▪ Normatividad NERC CIP

El grupo de estándares North American Electric Reliability Corp. Critical Infrastructure Protection (NERC CIP) [11] aprobado por FERC (Federal Energy Regulation Commision) fue creado para proteger el sistema eléctrico norteamericano de ataques ciberterroristas, se enfocan en la seguridad de ciber activos esenciales para la operación confiable del sistema eléctrico considerados infraestructura crítica y se formó para regular, hacer cumplir, monitorear, administrar la seguridad física y lógica de los sistemas que administran la energía eléctrica de las redes; los estándares son de carácter obligatorio para todas las

empresas que tienen activos críticos para el servicio esencial de energía (generación, transmisión, distribución) en Estados Unidos, esto incluye compañías de Canadá y México.

Actualmente los numerales de NERC CIP que están vigentes son:

- CIP-002-5.1aCyber Security BES Cyber System Categorization
- CIP-003-6 Cyber Security - Security Management Controls
- CIP-004-6 Cyber Security - Personnel & Training
- CIP-005-5 Cyber Security - Electronic Security Perimeter(s)
- CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems
- CIP-007-6 Cyber Security - System Security Management
- CIP-008-5 Cyber Security - Incident Reporting and Response Planning
- CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems
- CIP-010-2 Cyber Security - Configuration Change Management and Vulnerability Assessments
- CIP-011-2 Cyber Security - Information Protection
- CIP-014-2 Physical Security

Estos numerales o estándares evolucionan de manera independiente según las tendencias y el análisis del entorno en pro se deben cumplir en su totalidad en Norteamérica; en Colombia este estándar se implementa como buenas prácticas en compañías del sector eléctrico, entre ellas XM, para subir los niveles de seguridad de su infraestructura critica, actualmente, en Colombia está publicado el Acuerdo 788 Guía de Ciberseguridad (septiembre de 2015) el cual es una versión ajustada a las características del sistema interconectado Nacional de las normar americanas, debido a las diferencia entre países y los grados de madurez, aplica a las compañías del sistema interconectado nacional SIN que cuentan con infraestructura critica para la prestación del servicio de energía en Colombia, esta guía se basa NERC CIP v4 y especifica:

1. Es de carácter obligatorio para las compañías del SIN que cuenten con activos críticos.
2. Las compañías s deberán designar la persona responsable de dirigir y administrar la implementación de la Guía de Ciberseguridad.

3. El CNO definirá y estructurará un plan de trabajo que incluya actividades de sensibilización, comunicación, entrenamiento y socialización de la Guía de Ciberseguridad del CNO y de los procesos de seguridad cibernética que incluyan como mínimo aspectos como:
    - Identificación y documentación de la situación actual.
    - Establecimiento de procesos.
    - Diseño de arquitecturas detalladas.
    - Definición e implantación de controles mínimos legales, técnicos, organizativos y físicos.
    - Implementación de un ciclo de mejora permanente del proceso.

4. El operador del Sistema y los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional, deben realizar la identificación de los activos críticos y ciber activos críticos, los riesgos y vulnerabilidades y el nivel de gestión de ciberseguridad en la operación de sus empresas en un plazo máximo de (1) un año contado a partir de la fecha de expedición del presente Acuerdo.

XM por ser el operador del sistema interconectado nacional está en obligación de cumplir el acuerdo 788 y su más reciente actualización el acuerdo 1241[12], debido a su papel relevante en el ciclo energético se optó por seguir las versiones más actualizadas de NERC CIP ya descritas, por tal motivo el proyecto de supervisión avanzado debe cumplir dicha norma.

- **Nist Cibersecurity Framework (NCF): Framework for Improving Critical Infrastructure Cybersecurity**

Este framework surge de la solicitud expresa del presidente Barak Obama al NIST (National Institute of Standards and Technology) para dar respuesta al aumento de los ataques informáticos a las infraestructuras críticas norteamericanas, la primera versión se publica en 2014 y hoy existe una versión de 2018.

De acuerdo con el NIST [13] El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la

organización.

El framework está definido en términos de funciones y dividido en categorías y subcategorías, las funciones descritas son:

- Identificar (Identify): Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.
- Proteger (Protect): Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.
- Detectar (Detect): Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua.
- Responder (Respond): Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.
- Recuperar (Recover): Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

2.2 El estado del arte

Proyecto ISAAC propone la implementación de un sistema WAMPAC (Wide Área de Medición, Protección y Control System) para evitar o mitigar el impacto de los grandes eventos en el Sistema eléctrico Interconectado Colombiano, el proyecto se encuentra actualmente en fase de prototipo donde se trabaja con equipos diseñados para la medición fasorial (PMU). El proyecto se enmarca en la iniciativa Smart Grid de XM S.A. E.S.P. y no cuenta con una línea de ciberseguridad ni de seguridad informática. [5]. Estas misma deficiencia de ciberseguridad se ven reflejadas en material científicos como los estudios de ciberseguridad del sector eléctricos y los aportes realizados por Colombia inteligente

La Investigación sobre ciberseguridad en Colombia para el sistema eléctrico basado en la tecnología SCADA/EMS y supervisión mediante RTU (Unidad terminal remota) promueve la implementación de las mejores prácticas para el sector, con el fin de hacer frente a uno de los principales desafíos del siglo 21 como lo es el ciberterrorismo, esta investigación propone la implementación de normas como la NERC CIP versión 3, dicha norma es el estándar para sistema eléctrico norteamericano. Los conceptos asociados a norma NERC CIP todavía son válidos y el concepto de RTU es una aproximación del sistema actual.[17].

Colombia inteligente (Smart Colombia) es un programa no gubernamental cuyo objetivo es establecer diferentes estrategias para una implementación exitosa de tecnología de red inteligente en Colombia entre ellas se encuentra el proyecto ISAAC. Las preocupaciones ambientales, el aumento del consumo de electricidad, la seguridad del suministro de energía, la infraestructura obsoleta y los significativos avances en las tecnologías de comunicación e información se han identificado como los principales para elementos para despliegues de redes inteligentes. Plantea la incorporación de las PMU en la supervisión del sistema eléctrico colombiano, la cual no contempla temas de ciberseguridad [18].

La inclusión de sincrofasores (PMU) a las redes eléctricas mejoran el monitoreo en tiempo real y el análisis de eventos de las subestaciones eléctricas, brindando información mucho más completa para las tareas de supervisión de los centros de control. Los Sincrofasores soportan su operación en redes de comunicaciones IP (vulnerables) y elementos de almacenamiento de tipo big data. Al ser dependientes de las redes de comunicación IP se pueden encontrar en ellos gran número de vulnerabilidades asociadas a ciberseguridad y seguridad tecnológica. Así mismo los modelos de convergencia de redes de tecnología (TI) con tecnologías de operación (TO) suman grandes riesgo a la operación.

La integración entre sistemas de información y sistemas de operación(control industrial) es una tendencia a nivel mundial, estas tendencias incrementan el riesgos desde el punto de vista de diseño y desarrollo de sistemas que manejan información crítica, la ciberseguridad física juega un papel importante en la protección de los activos críticos, esta investigación presenta un modelo que ayuda a determinar los factores de mitigación de los niveles de riesgo y propone un método para contener adecuadamente y minimizar tales riesgos [19]. Para poder mitigar estos riesgos se han venido desarrollando estrategias en el control y la operación de sistemas en tiempo real en las redes WAMS, las cuales requieren de un sistema rentable de altas velocidades y comunicaciones seguras, esto se ha convertido en los nuevos retos de la ciberseguridad, se propone la arquitectura de seguridad cibernética para las redes eléctricas grid y se comienza a valida el impacto en la latencia del cifrado de las comunicaciones con protocolos como IPSEC. [20].

Por otro lado, la literatura ya hablada de ataques informáticos en ambientes controlados por el personal científico [21][22][23], en dónde se establecen que muchos de los ataques tienen una alta probabilidad de ocurrencia, con ello, los sistemas industriales estarían en alto riesgo si los eventos de ciberseguridad se materializan.. los taques referenciados en dicha documentación se basan en: la negación de servicios, la lectura de la operación o la escritura de comandos (comand and control), esta misma literatura indica algunas protecciones o controles a nivel de accesos y cifrado, así como el análisis de protocolos específicos de sistemas de control industrial como ICCP y la utilización de protocolos de comunicación específicos para PMU IEEE C37.118; Actualmente el proyecto ISAAC está en definición de su red de comunicaciones y utiliza el protocolo IEEE C37.118, sin embargo, es necesario integrar la información e las diferentes amenazas, vulnerabilidades y controles para la mitigación, a través de un modelo que integre los distintos hallazgos de la literatura como: el desarrollo de plataformas de simulación y co-simulación , el uso de tecnologías

baso de Deep Learning, utilización de algoritmos bayesianos, los modelos de censado, modelo de balanceo y protección, la definición de algoritmos matemáticos, los modelos de evaluación de riesgo y el análisis detallado de protocolos industriales [24][25][26][27][28][29][30][31][32][33][34][35][36][37].

Las vulnerabilidades referenciadas por los distintos autores sobre dispositivos PMU son:

- Ataques inobservables o imperceptibles, ataques de denegación de servicios, ataques de denegación de servicios distribuidos los cuales afecta directamente la disponibilidad de los dispositivos tipo PMU, se demuestran patrones y modelos matemáticos basados en equipos estándar del mercado y redes de comunicaciones que utilizan servicios de IP [38] [39] [40][41][42][43].

- Acceso y manipulación indebida de dispositivos, ataques de escucha de datos o manipulación de datos (Hombre en el medio) el cual es el ataque más común para los dispositivos PMU, por medio de estos tipos de ataques se puede alterar las lecturas o el funcionamiento normal de los equipos o manipularla inyectando una gran cantidad de datos erróneos que afectan directamente la prestación del servicio de supervisión y operación [44][45][46] [47] [48][49][50][51][52][53] [54][55][56].

- Ataques de manipulación de relojes y manipulación de sincronización de GPS, cuando se habla de sistemas en tiempo real basados en PMU es muy importante contar con lecturas o datos en milisegundos y que deben estar sincronizadas, cuando se presenta una desviación o retardo en las medidas se inyectan datos erróneos al sistema, los distintos autores han demostrado como se puede afectar el sistema por medio de la manipulación de los relojes o GPS, se debe contemplar este tipo de ataque aunque no afecte el funcionamiento de la PMU y se debe validar la posibilidad de presentarse en el modelo de ISAAC [57][58][59][60] [61].

Todos estos análisis de vulnerabilidades y documentación de tipos de Ataques sobre PMU aporta un marco de referencia importante, pero se debe tener presente que todos están basados en equipos comerciales y redes de comunicaciones estándares, el proyecto ISAAC cuenta actualmente con aproximadamente 40 PMU tipo prototipo que fueron diseñadas por grupo de investigación de XM y no cuenta con las características específicas de los estudios realizados, adicionalmente, no se habla de modelos de protección debido a que estos temas son clasificados como confidenciales por la compañía del sector eléctrico a nivel mundial.

En el ámbito mundial ya se conocen ataques a infraestructuras críticas que soportan sistemas eléctricos, aunque ninguno de ellos en el ámbito de la PMU, los ataques y alertas más conocidos son:

- Ataque al sistema eléctrico de Ucrania, en los años 2015 [62] y 2016 [63] impactando centrales de distribución y utilizando técnicas de suplantación en correo por medio del cual lograron acceder a los sistemas de TI y posterior con técnicas avanzadas de

escalamiento de privilegios tomaron control de los SCADA y lograron generar apagón en un porcentaje del país, demostrando así que los equipos de control de industrial es posible alcanzarlos.

- Los constante reportes de alertas emitidos por las centrales de inteligencia mundial y en especial el US-CERT, dan muestra que los sistemas eléctrico son objetivo de ataque para gobiernos y grupos especializados, en ellos se destaca: CrashOverride es un malware que ataca sistemas SCADA en organizaciones que utilizan los protocolos IEC101, IEC104, IEC61850 y OPC [64] las infiltraciones rusas sobre infraestructura critica americana el cual ya fue demostrado y aceptado por el gobierno norteamericano[65], las botnet como hidden cobra diseñadas para hacer denegación de servicios sobre infraestructuras críticas [66], los reportes de Amenazas Persistentes avanzadas [67] sobre sector eléctrico y otros sectores en estados Unidos, en nuestro país los resientes ataques de DOS y malware avanzado sobre empresas de infraestructura critica reportadas por el CSIRT de gobierno el 29 de octubre de 2018, Lo que demuestra que existen grupos organizados y gobiernos dedicados a generar eventos o incidentes sobre las infraestructuras críticas de las cuales hace parte las PMU, de no implementar controles en la PMU, prontamente estos u otros ataques podrán permear estos dispositivos y generar afectación en al sistema eléctrico nacional.
- La petrolera Mexicana Pemex en noviembre de 2019 sufrió un ataque de ransomware en varias estaciones de trabajo (5% de sus equipos), para lo cual, los delincuentes exigieron un pago de 565 bitcoin (equivalente a 5 millones de dólares), diferentes portales especializados en temas de seguridad establecieron una criticidad alta ante éste evento y marcó un hito en las industrias que operan infraestructuras críticas con respecto a los ciberataques [68] [69] [70].

3. Metodología

La metodología por medio de la cual se lograron los objetivos fue dividida en fases:

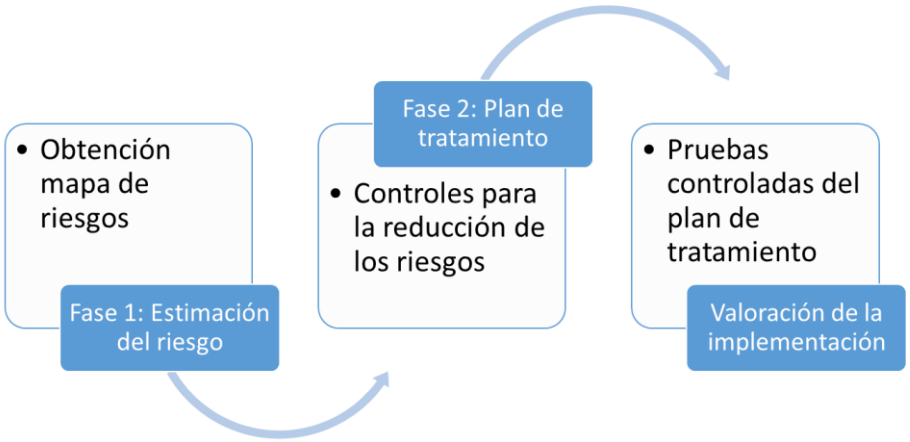


Figura 3 Metodología para el cumplimiento de objetivos. Fuente propia

Para el proceso de riesgos, se usó un archivo Excel de propósitos académicos entregado desde el programa de la maestría en seguridad.

3.1 Fase 1: Estimación de riesgos

El proceso para la obtención de los riesgos se realizó con base en la norma ISO 27005:2018 como proceso fundamental, para lo cual, ejecutaron los siguientes pasos en esta fase:

1. **Establecer el contexto**. Es la definición del contexto del riesgo y dentro de éste, el alcance.
2. **Identificación de riesgos**:

   Dentro de este subproceso se realizaron las siguientes actividades:

   i. Se realizó el levantamiento de activos de información, que permita conocer las amenazas y vulnerabilidades del sistema, esto es a través de entrevistas con expertos y descubrimiento automática en la red.

   ii. Así mismo, se realizó una revisión de las condiciones y marcas de los diferentes activos.

   iii. Se realizó un inventario de amenazas técnicas.

   iv. Como parte de la identificación de activos, se realizó una prueba (descubrimiento de activos) con ello, se obtuvo un mapa técnico del inventario.

v. Sse realizó una prueba de seguridad controlada, con el fin de identificar posibles vulnerabilidades técnicas (vectores de ataque). Algunos de los ataques ejecutados fueron:

- Enumeración: puertos, servicios, vulnerabilidades web.
- De fuerza bruta o diccionario.
- Denegación de servicios.
- Escalamiento de privilegios.
- Hombre en el medio.
- Desplazamiento lateral.
- Envenenamiento de red.
- Inyección de código.
- Suplantación de usuarios o equipos.
-

Para el levantamiento de activos, se usó la tabla 1, se consideraron las siguientes características

Tabla 1 Modelo para levantamiento de información

Inventario de PMU y servidores					
#	**Tipo**	**Departamento**	**Marca**	**S.O.**	**red**

Después de entrevista con el grupo de trabajo del Proyecto ISAAC, se entrega inventario de PMU y servidores que lo componen, este inventario presenta los siguientes campos:

- **# Equipos**: Enumeración de equipos
- **Tipo:** Se encuentran dos tipos, PMU y servidores para operación de las PMU
- **Departamento:** Sitio de ubicación geográfica, se describe a nivel de departamento por la confidencialidad de la información.
- **Marca:** Se especifica las marcas de las PMU utilizadas en el proyecto, para aquellos equipos desarrollado por el proyecto se marcan como prototipo.
- **Sistema Operativo:** Indica el proveedor de sistema operativo con que cuentan las PMU, la versión de este no es posible detallarla por temas de confidencialidad, para las PMU comerciales se indica como propietario.

Finalmente se construye tabla 2 donde se indica el tipo de ataque realizado sobre los distintos activos y su impacto en la red

Tabla 2: Tipos de ataques vs dispositivos e impacto

Ataques realizados	Dispositivos	Impacto

Fuente propia.

3. Análisis de riesgos

Ya con los activos de información y las diferentes amenazas:

i) Se obtuvieron los vulnerabilidades y controles actuales que cada activo tiene, con ello, poder establecer la probabilidad y los posibles impactos generados en el momento de materializarse alguna de las amenazas. Para obtener el nivel de efectividad de los controles, se tomó la siguiente escala de valoración en porcentaje los cuales se ven en la tabla 3.

Tabla 3 Porcentajes de valoración de cumplimiento de controles

Porcentaje	Descripción
0%	No se cuenta con controles.
25%	Algunos controles están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo).
50%	todos los controles propuestos están implementados, pero no se valida su efectividad.
75%	Todos los controles están implementados, se verifican su efectividad, pero no se monitorea ni se hacen planes de mejora continua.
100%	La totalidad de controles están implementados, se miden, monitorean y se generan planes de acción para su mantenimiento (líneas bases periódicas y auditorias).

Fuente propia.

Es importante precisar que ésta escala de valoración de controles en una guía, por lo cual, es posible tener calificaciones ponderadas entre 2 valores, por ejemplo, es posible dar la calificación de 35%.

ii) Se hizo un cruce de escenarios con el fin de obtener la aplicabilidad en consideración de los posibles impactos sobre los activos. Para dicho cruce, se hace una selección de “X” acorde a la aplicabilidad de la amenaza sobre el activo en a tabla 4:

Tabla 4 Modelo de levantamiento de amenazas

ACTIVOS AMENAZAS	Activo 1	Activo 2	Activo 3	Activo 4
Amenaza 1	x	x	**x**	
Amenaza 2			**x**	**x**

Fuente propia

4. **Evaluación de riesgos**

   Se realizó la definición de las tablas de probabilidad e impacto, como factor de impacto se seleccionó la afectación en la operación, en consideración que el análisis desarrollado es sobre una infraestructura crítica, por lo cual, la disponibilidad es un factor fundamental.

   Las tablas 5 y 6 de probabilidad e impacto respectivamente utilizadas son las siguientes:

Tabla 5 Probabilidad/ Frecuencia

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Raro**	Puede ocurrir solo bajo circunstancias excepcionales.
2	**Improbable**	Podría ocurrir algunas veces.
3	**Posible**	Puede ocurrir en algún momento.
4	**Probable**	Probabilidad de ocurrencia en la mayoría de las circunstancias.
5	**Casi seguro**	La expectativa de ocurrencia se da en la mayoría de las circunstancias.

Fuente propia

Tabla 6 Impacto en la operación sobre los activos

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Insignificante**	Hay una indisponibilidad de plataforma o de la información menor a 4 y la puede resolver la mesa de ayuda.
2	**Menor**	Hay una indisponibilidad de plataforma o de la información entre 4 y 12 horas, es necesario escalarlo a 2 nivel.
3	**Intermedio**	Hay una indisponibilidad de plataforma o de la información entre 12 y 36 horas, se requiere consulta el proveedor.
4	**Mayor**	Hay una indisponibilidad de plataforma o de la información entre 36 y 72 horas, se requiere al proveedor en sitio.
5	**Superior**	Hay una indisponibilidad de plataforma o de la información por más de 72 horas, es necesario establecer un mecanismo de procesamiento alterno.

Fuente propia

Como el proyecto se encuentra en etapa de investigación solo se mide su impacto en términos e indisponibilidad de plataforma o de la información.

La calificación de los riesgos se realiza acorde al escenario entregado en la figura 4:

No.	Escenario de riesgos	PROBABILIDAD		IMPACTO OPERACIÓN	
(1)	Posibilidad que la amenaza: Amenaza 1, afecte el activo: Activo 1	Posible	3	Mayor	4
(2)	Posibilidad que la amenaza: Amenaza 1, afecte el activo: Activo 2	Probable	4	Insignificante	1
(3)	Posibilidad que la amenaza: Amenaza 1, afecte el activo: Activo 3	Posible	3	Menor	2
(4)	Posibilidad que la amenaza: Amenaza 2, afecte el activo: Activo 3	Posible	3	Superior	5
(5)	Posibilidad que la amenaza: Amenaza 3, afecte el activo: Activo 1	Probable	4	Mayor	4

Figura 4 Calificación escenarios de riesgos: probabilidad e impacto. Fuente propia

Finalmente, al calificar todos los riesgos, se obtiene el mapa de riesgos figura 6, el cual considera 4 zonas como se aprecia en la figura 5:

ZONA	
Aceptable	Riesgo bajo, se administra con procedimientos rutinarios
Tolerable	Riesgo moderado, la responsabilidad gerencial debe ser especificada
Inaceptable	Riesgo Alto requiere atención de la alta gerencia
Inadmisible	Riesgo Extremo, se requiere acción inmediata

Figura 5 Definición de las zonas de aceptabilidad. Fuente propia

	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3					
Improbable	2					
Raro	1					

Figura 6 Mapa de aceptabilidad acorde a la calificación del riesgo Fuente propia.

3.2 Fase 2: Definición del plan de tratamiento.

En esta fase se ha dividido en 2 actividades:

3.2.1 Actividad 1: Plan de tratamiento

1. **Homologación de normas:**

Se realizó homologación de reglas la cual consistió en realizar el cruce de las distintas normas, Se toma como base la norma Nist Cibersecurity Framework (NCF) la cual es la norma para las infraestructuras críticas, posteriormente se realiza cruce de las normas ISO 27001:2013 y de las NERC CIP en sus versiones actuales. Pare esto se utilizó la siguiente plantilla de la tabla 7:

Tabla 7 Modelo levantamiento de cruce información de Normas

Nist Cibersecurity Framework		Numeral ISO 27001	Numeral NERC Cip
Identificar	ID-AM		
	ID-AM		
	ID-AM		
Proteger	PR-		
	PR-		
	PR-		
Detectar	DE-		
	DE-		
	DE-		
Responder	RS-		
	RS-		
	RS-		
Recuperar	RC-		
	RC-		
	RC-		

Fuente propia

2. **definición de planes:**

Para todos los riesgos detectados se definió uno o varios planes de tratamiento. Los planes deben estar basados en la homologación de las normas realizadas en el numera anterior, los planes se definirán en el siguiente formato de la tabla 8:

Tabla 8 Modelo de descripción de planes

Nombre del plan	
Descripción	
Activos afectados	
Riesgos mitigados	

tecnología a implementar	

Fuente propia

3.2.2 Actividad 2: Modelo de ciberseguridad

Con base en la homologación de las normas, los planes de tratamiento, riesgos asociados y la arquitectura actual del proyecto, se realizó un modelo de ciberseguridad para la red de supervisión futura, este plan al seguirlo minimizará el riego cibernético y mejorará la capacidad de respuesta ante incidentes cibernéticos para la red de supervisión

El modelo se realizó siguiendo el formato de la tabla 9

Tabla 9: Estructura del modelo de ciberseguridad de las PMU

Modelo de ciberseguridad basado en Nist Cibersecurity Framework, ISO 27001:2013 y NERCCIP		
Identificar	a	
	b	
	c	
Proteger	a	
	b	
	c	
Detectar	a	
	b	
	c	
Responder	a	
	b	
	c	
Recuperar	a	
	b	
	c	

Fuente propia

3.3 Fase 3: Valorar la implementación del modelo

3.3.1 Actividad 1: verificación del ambiente de pruebas

Como parte importante para la validación de la implementación y el nivel de riesgo de controles, es importante evidenciar cómo se encuentra el ambiente de pruebas y cuáles fueron los cambios significativos que se agregaron a esta red.

Para este ambiente se dispuso de un nuevo servidor *alienvault* por medio del cual se realizó un escaneo para identificar el inventario de activos en la red.

3.3.2 Actividad 2: Implementación de controles

Una vez definidos los planes se procedió a la implementación de controles sobre los riesgos altos (amarillos y rojos), se diligencia la tabla 10 la cual indica el estado de los controles y su nivel de cumplimiento, algunos de los controles administrativos se dejan propuestos.

Tabla 10: Modelo resumen de implementación de planes:

Nombre plan	Porcentaje implementado	Que se ha implementado	Que falta implementar	Fecha probable implementación

Fuente propia

3.3.3 Actividad 3: Validación de controles

Una vez validado el estado de implementación de controles se procede nuevamente a realizar evaluación de riesgos.

Se realizó validación similar a la realizada en el numeral Fase 1: Estimación de riesgos, para lo cual, se ejecutó una prueba técnica de seguridad de acuerdo con los vectores de ataques definidos, se comparó con el análisis de riesgos iniciales y se validaron los siguientes numerales:

1. Identificación de riesgos:
2. Análisis de riesgos
3. Evaluación de riesgos
4. Cuadro comparativo de hallazgos de la Fase 1: Estimación de riesgos

Al final se realiza cuadro comparativo de resultados en el cual se expone el antes y el después de implementar controles definidos en el modelo de ciberseguridad de las PMU:

5. Cuadro comparativo de diagramas de calor
6. Cuadro comparativo de diagrama de tortas de riesgo

4. Resultados

4.1 Fase 1: Estimación de riesgos

4.1.1 Establecimiento del contexto

En consideración de este proyecto de grado, el contexto es el ambiente aislado de laboratorio el cual permite utilizar el ambiente pruebas del proyecto de manera controlada, instalar equipos de seguridad y equipos para hacer pruebas controladas, incluyendo ataques sobre las PMU y elementos de infraestructura, adicionalmente las pruebas más intrusivas se realizaron con PMU tipo prototipo aisladas y desconectadas de la red pero con la misma características de las de los ambientes de pruebas y producción, estas pruebas fueron realizadas por el personal que estaban a cargo de este proyecto de tesis y con la supervisión de los líderes del proyecto de supervisión futura.

4.1.2 Identificación de los riesgos

a) Levantamiento de activos con los líderes del proyecto:

La red de ISAAC cuenta con distintos segmentos los cuales sirven para varias investigaciones de este, es de resaltar que hoy se cuenta con una estrategia de segmentación basada en segmentación de redes y separada por firewall para independizar el ambiente de los ambientes corporativos, aunque existen equipos del ambiente corporativo que tienen la capacidad de interactuar con el proyecto, la figura 7 muestra la segmentación:

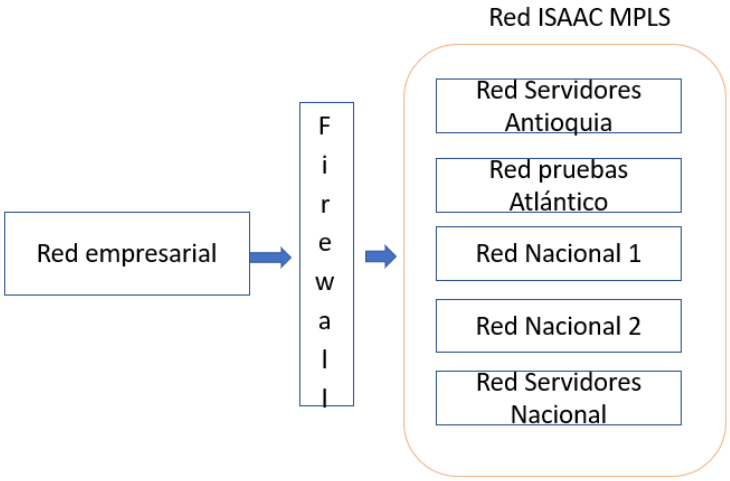


Figura 7: Esquemático de red. Fuente propia

Se realiza una breve descripción de las redes para su contexto:

- **Red empresarial:** En esta red se encuentran servidores o equipos que se interactúan con la red de PMU
- **Firewall:** Equipo barrera para independizar las redes de investigación
- **Red Servidores Antioquia:** Red de servidores que concentran las lecturas de todas las PMU.
- **Red Pruebas 1** Atlántico: red de PMU ubicadas en el departamento del atlántico
- **Red Nacional 1:** Red de PMU a nivel nacional del proyecto ISAAC
- **Red Nacional 2:** Red de PMU a nivel nacional hacen parte del piloto de redes distribuidas
- **Red servidores Nacional**: prototipo de servidores distribuidos

A continuación (tabla 11) se encuentra el listado de activos de información obtenidos, para lo cual, en consideración que se trata de información actual y activa, algunas de las versiones de los sistemas no se brindan, por temas de seguridad (confidencialidad).

Tabla 11 : inventario de equipos resultado de reunión con el personal proyecto

Inventario de PMU y servidores					
#	**Tipo**	**Departamento**	**Marca**	**S.O.**	**red**
1	PMU	Huila	Prototipo	Windows	Red Nacional 1
2	PMU	Norte de Santander	Comercial 1	Propietario	Red Nacional 1
3	PMU	Cundinamarca	Comercial 2	Propietario	Red Nacional 1
4	PMU	Cundinamarca	Prototipo	Windows	Red Nacional 1
5	PMU	Cundinamarca	Prototipo	Windows	Red Nacional 1
6	PMU	Córdoba	Prototipo	Windows	Red Nacional 1
7	PMU	Antioquia	Prototipo	Windows	Red Nacional 1
8	PMU	Risaralda	Prototipo	Windows	Red Nacional 1
9	PMU	Valle del Cauca	Prototipo	Windows	Red Nacional 1
10	PMU	Bolívar	Prototipo	Windows	Red Nacional 1
11	PMU	Córdoba	Prototipo	Windows	Red Nacional 1
12	PMU	Manizales	Prototipo	Windows	Red Nacional 1
13	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
14	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
15	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
16	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
17	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
18	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico

19	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
20	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
21	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
22	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
23	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
24	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
25	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
26	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
27	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
28	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
29	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
30	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
31	PMU	Atlántico	Comercial 3	Propietario	Red pruebas Atlántico
32	PMU	Atlántico	Prototipo	Windows	Red pruebas Atlántico
33	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
34	PMU	Atlántico	Comercial 2	Propietario	Red pruebas Atlántico
35	PMU	Cundinamarca	Comercial 2	Propietario	Red Nacional 1
36	PMU	Córdoba	Comercial 2	Propietario	Red Nacional 1
37	PMU	Córdoba	Prototipo	Windows	red nacional 2
38	PMU	valle del cauca	Prototipo	Windows	Red Nacional 1
39	PMU	Boyacá	Comercial 4	Propietario	red nacional 2
40	PMU	Risaralda	Comercial 4	Propietario	red nacional 2
41	PMU	Norte de Santander	Comercial 4	Propietario	red nacional 2
42	PMU	Santander	Comercial 4	Propietario	red nacional 2
43	PMU	Valle del auca	Comercial 4	Propietario	red nacional 2
44	PMU	Tolima	Comercial 4	Propietario	red nacional 2
45	PMU	Córdoba	Comercial 4	Propietario	red nacional 2
46	PMU	Córdoba	Comercial 4	Propietario	red nacional 2
47	PMU	Meta	Comercial 4	Propietario	red nacional 2
48	PMU	Santa Rosa, Bolívar	Comercial 4	Propietario	red nacional 2
49	PMU	Cundinamarca	Comercial 4	Propietario	red nacional 2
50	PMU	cesar	Comercial 4	Propietario	red nacional 2
51	PMU	Antioquia	Comercial 4	Propietario	red nacional 2
52	PMU	Nariño	Comercial 4	Propietario	red nacional 2
53	PMU	Antioquia	Comercial 4	Propietario	red nacional 2
54	PMU	Boyacá	Comercial 2	Propietario	red nacional 2
55	PMU	Cundinamarca	Comercial 2	Propietario	red nacional 2
56	PMU	Nariño	Comercial 2	Propietario	red nacional 2
57	PMU	Antioquia	Comercial 2	Propietario	red nacional 2
58	PMU	Atlántico	Comercial 2	Propietario	red nacional 2
59	PMU	Boyacá	Comercial 4	Propietario	red nacional 2
60	PMU	Boyacá	Comercial 4	Propietario	red nacional 2
61	PMU	Vichada	Comercial 4	Propietario	red nacional 2

62	PMU	Norte de Santander	Comercial 4	Propietario	red nacional 2
63	PMU	Antioquia	Comercial4	Propietario	red nacional 2
64	PMU	Antioquia	Comercial 4	Propietario	red nacional 2
65	servidor 1	Antioquia	N/A	Windows	Red Servidores Antioquia
66	servidor 2	Antioquia	N/A	Windows	Red Servidores Antioquia
67	servidor 3	Antioquia	N/A	Windows	Red Servidores Antioquia
68	servidor 4	Antioquia	N/A	Windows	Red Servidores Antioquia
69	servidor 5	Antioquia	N/A	Linux	Red Servidores Antioquia
70	servidor 6	Antioquia	N/A	Windows	Red Servidores Antioquia
71	servidor 7	Antioquia	N/A	Windows	Red Servidores Antioquia
72	servidor 8	Antioquia	N/A	Windows	Red Servidores Antioquia
73	servidor 11	Atlántico	N/A	Windows	Red pruebas Atlántico
74	servidor 12	Atlántico	N/A	Windows	Red pruebas Atlántico
75	servidor 13	Atlántico	N/A	Windows	Red pruebas Atlántico
76	servidor 14	Atlántico	N/A	Windows	Red pruebas Atlántico
77	servidor 15	Atlántico	N/A	Windows	Red pruebas Atlántico
78	servidor 16	Atlántico	N/A	Windows	Red pruebas Atlántico

Fuente propia

Del inventario entregado por el proyecto, se evidencia que existente 64 PMU con distribución nacional, de las cuales 13 son tipo prototipo (desarrollas por XM, computadores industriales con sistema operativo Windows, con desarrollo a la medida para hacer las funciones similares a las PMU comerciales) y 51 marcas comerciales, esto es, PMU que tienen un sistema operativo propietario.

b) *Levantamiento de inventario con descubrimiento automático*

Con el objetivo de validar con más exactitud la cantidad de activos de información se instaló un servidor *OSSIM alienvault*, con éste, se activó la funcionalidad de descubrimiento automático, así, poder cotejar esta información con el inventario ya levantado. Para ello, se realizaron las siguientes configuraciones en:

- Configuración de reglas de firewall para su administración.
- Enrutamiento de redes para poder visualizar cada uno de los segmentos de la red ISAAC.
- Configuración de salida a internet del servidor para permitir sus actualizaciones.
- Configuración de perfiles y acceso sobre el servidor.

Una vez se configuró el servidor, se procede a realizar el escaneo de red teniendo las precauciones necesarias para no afectar el performance de la red y se detecta varios equipos distintos a los reportados por el proyecto, el detalle de estos se presenta en la tabla 12:

Tabla 12 : Nuevos equipos descubiertos: escaneo por herramienta especializada

Inventario de equipos después de realizar escaneo					
#	**Tipo**	**Departamento**	**Marca**	**SO**	**RED**
1	eq comunicación	Antioquia		Propietario	Red servidores
2	eq comunicación	sin identificar		Propietario	red nacional 1
3	eq comunicación	sin identificar		Propietario	red nacional 1
4	eq comunicación	sin identificar		Propietario	red nacional 2
5	eq comunicación	sin identificar		Propietario	red nacional 2
6	eq comunicación	sin identificar		Propietario	red nacional 2
7	equipo industrial	Atlántico		Propietario	red Atlántico
8	equipo industrial	Atlántico		Propietario	red Atlántico
9	equipo industrial	Atlántico		Propietario	red Atlántico
10	firewall	Antioquia		Propietario	red servidores nacional
18	PMU	Cesar	Comercial 5	Propietario	red nacional 1
19	PMU	Atlántico	Comercial 2	Propietario	red nacional 2
20	PMU	Cesar	Comercial 5	Propietario	red nacional 1
21	PMU	Pasto	Comercial 2	Propietario	red nacional 2
22	PMU	Caldas	Comercial 2	Propietario	red nacional 2
23	router	Antioquia		Propietario	red servidores Antioquia
27	servidor	Antioquia		Linux	red servidores Antioquia
28	servidor	Antioquia		Linux	red servidores Antioquia
29	servidor	Antioquia		Linux	red servidores Antioquia
30	servidor	Norte Santander		Windows	red servidores nacional
31	servidor Alienvault	Antioquia		Linux	red servidores Antioquia

Fuente propia

De estos equipos encontrados se destaca que existen 5 PMU no reportadas y distribuidas en las distintas redes, se evidencia que se cuenta con PMU con marca comercial 5.

Adicional a esto, con los resultados del escaneo, se evidencia que los proyectos no tienen un control total de los activos y que por las configuraciones y características de cada uno de los segmentos es posible conectar equipos en cada una ellas según los planes de trabajo de la investigación, lo cual representa un alto riesgo en toda la red.

Con la información recolectada este trabajo se enfocó en 69 PMU en total con distribución nacional entre la cuales se tienen PMU comerciales y prototipo.

Adicional a las PMU, se tienen los siguientes activos de información, los cuales hacen parte del sistema ISAAC:

- Router
- Firewall
- Switch

- Servidores recepción
- Personas
- Información
- Sedes operador
- Sedes agentes del SIN
- Cableado Operador
- Cableado agentes del SIN

En conclusión, se obtuvieron 12 activos de información, en consideración que se unifican las PMU en 2 grupos, las comerciales y las se sistema operativo tipo Windows.

c) *Posibles amenazas sobre los activos de información.*

A continuación (tabla 13), se puede apreciar el listado de amenazas posibles que pueden afectar los activos de información:

Tabla 13 Listado de amenazas

Listado amenazas
Acceso Físico No Autorizado
Acceso Lógico No Autorizado
Apt
Arp Poison
Arp Spoofing
Ataque De Diccionario O Fuerza Bruta
Ataque DOS Y DDOS
Ataque Ntp (Desincronización)
Ataque Sqlinyection
Ataque Web
Código Malicioso
Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.)
Conflictos personal proyecto
Envenenamiento De XML
Exploit
Ingeniería Social
Interceptación De Cableado
Daño Cableado Estructurado
Manipulación De Datos
Obsolescencia Técnica Y Tecnológica
Password Craking
Perdida O Fuga De Información
Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.)
Ransomware
Rotación O Cambio De Personal Gestor Del Proyecto
Saturación De Direcciones Mac O Ataques De Flooding De Mac.
Scanning
Suplantación De Identidad
Suplantación De Señales De Control

XSS

Fuente propia

d) Ataques realizados sobre grupos de activos e impacto

Finalmente se construye tabla 14 donde se indica el tipo de ataque realizado sobre los distintos activos y su impacto en la red

Tabla 14 Tipos de ataques vs dispositivos e impacto

Ataques realizados	***Activos***	**Impacto**
Enumeración: puertos, servicios, vulnerabilidades web.	• PMU comercial • PMU prototipo • Router • Firewall • Switch • Servidores recepción	Medio Es posible realizar escaños y tener los detalles de vulnerabilidades de los distintos dispositivos
Ataque De fuerza bruta o diccionario.	• PMU comercial • PMU prototipo • Router • Firewall • Switch • Servidores recepción	Alto Es posible tener la credenciales de equipos, logrando escalado de privilegios
Denegación de servicios	• PMU comercial • PMU prototipo • Servidores recepción	Alto Es posible hacer ataques de denegación de servicios que los pone no disponible
Escalamiento de privilegios y Desplazamiento lateral.	• PMU comercial • PMU prototipo • Servidores recepción	Alto Es posible moverse entre usuarios en distintos dispositivos, logrando escalar permisos.
Hombre en el medio.	• PMU comercial • PMU prototipo Servidores recepción	Medio Es posible hacer hombre en el medio, interceptado comunicaciones e identificando información relevante
Envenenamiento de red	• Switch	Medio: Es posible suplantar dispositivos conectados en la red
Inyección de código.	• PMU comercial • PMU prototipo • Servidores recepción	Alto Es posible hacer inyección de código, suplantando las medidas y las comunicaciones
Suplantación de usuarios o equipos.	• PMU comercial • PMU prototipo	Alto

	• Servidores recepción • Personas	Es posible suplantar usuarios debido a su bajo nivel de complejidad o a la falta de una línea base de seguridad
Phishing, ingeniería social	• Personas	Alto Es posible hacer robo de información e inteligencia sobre los usuarios, revelando datos importantes de los equipos
Interceptación de cableado y acceso a red	• Sedes operador • Sedes agentes del SIN • Cableado Operador • Cableado agentes del SIN	Medio Es posible tener acceso a los elementos físicos, de las sedes donde están implementadas las PMU

Fuente propia.

4.1.3 Análisis de riesgos

A continuación, en las tablas 15 al 26, se entregan las diferentes vulnerabilidades por activo, así como los controles actuales y el nivel de efectividad de dichos controles (calculado acorde a la tabla definida en la metodología):

Tabla 15 Vulnerabilidades, controles y nivel de efectividad. PMU con S.O comercial

PMU con S.O comercial		
Vulnerabilidades	**Controles actuales implementados**	**Efectividad de los controles**
Falta de actualizaciones firmware configuraciones por defecto Uso de protocolo débiles Web service vulnerables Falta segregación de funciones Controles de acceso débiles Falta de controles de auditoria Acceso a terceros para soporte no controlado Puertos físicos activos Uso de protocolos de comunicaciones inseguros usuarios por defecto Falta de cifrado	control físico control perímetro (firewall) red interna no publica	25%

Fuente propia

Tabla 16 Vulnerabilidades, controles y nivel de efectividad. PMU S.O Windows

PMU S.O Windows		
Vulnerabilidades	**Controles actuales implementados**	**Efectividad de los controles**
Sistema operativo obsoleto Falta de actualizaciones configuraciones por defecto	control físico control perímetro (firewall) red interna no publica	20%

Falta de Antivirus Uso de protocolo débiles Fallas de seguridad en acceso remoto Uso de protocolo smbv1 Exploit conocidos Falta de monitoreo Falta segregación de funciones Controles de acceso débiles Falta de controles de auditoria sql injection Acceso a terceros para soporte no controlado Ataques de día cero Puertos físicos activos (USB) Ataques a la cadena de suministro Uso de protocolos de comunicaciones inseguros Web service vulnerables Falta de cifrado		

Fuente propia

Tabla 17 Vulnerabilidades, controles y nivel de efectividad Router

Router		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
Falta de actualizaciones firmware configuraciones por defecto Uso de protocolo débiles Acceso a terceros para soporte no controlado falta de monitoreo de seguridad	control físico control perímetro administración por tercero Líneas base seguridad Segregación de funciones monitorio de plataforma	65%

Fuente propia

Tabla 18 Vulnerabilidades, controles y nivel de efectividad Firewall

Firewall		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
Falta de actualizaciones firmware configuraciones por defecto Uso de protocolo débiles Acceso a terceros para soporte no controlado arp spoofing falta de monitoreo de seguridad existencia de reglas tipo any entre redes	control físico control perímetro administración por tercero Línea base seguridad Segregación de funciones monitorio de plataforma Configuraciones personalizadas a puertos y servicios en las reglas	65%

Fuente propia

Tabla 19 Vulnerabilidades, controles y nivel de efectividad Switch

Switch		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**

Falta de actualizaciones firmware configuraciones por defecto Uso de protocolo débiles Acceso a terceros para soporte no controlado arp spoofing falta de monitoreo de seguridad	control físico control perímetro administración por tercero Línea base seguridad Segregación de funciones monitorio de plataforma	40%

Fuente propia

Tabla 20 Vulnerabilidades, controles y nivel de efectividad Servidores recepción

Servidores recepción		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
Falta de actualizaciones configuraciones por defecto Falta de Antivirus Uso de protocolo débiles Fallas de seguridad en acceso remoto Uso de protocolo smbv1 Exploit conocidos Falta de monitoreo Falta segregación de funciones Controles de acceso débiles Falta de controles de auditoria sqlinjection Acceso a terceros para soporte no controlado Ataques de día cero Puertos físicos activos (USB) Ataques a la cadena de suministro Uso de protocolos de comunicaciones inseguros Web service vulnerables Falta de cifrado	control físico control perímetro. Segmento independiente de servidores Líneas base seguridad	50%

Fuente propia

Tabla 21 Vulnerabilidades, controles y nivel de efectividad Personas

Personas		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
Falta de conocimiento en seguridad Ingeniería social	Cláusulas de confidencialidad concientización	0%

Fuente propia

Tabla 22 Vulnerabilidades, controles y nivel de efectividad Información

Información		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
interceptación de datos falta de controles de integridad falta de monitoreo	control físico Control perímetro	25%

Tabla 23 Vulnerabilidades, controles y nivel de efectividad Sedes operador

Sedes operador		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
falta de control de acceso falta monitoreo del proveedor Condiciones físicas adversas	Control físico Cableado estructurado datacenter	80%

Fuente propia

Tabla 24 Vulnerabilidades, controles y nivel de efectividad Sedes agentes del SIN

Sedes agentes del SIN		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
falta de control de acceso falta monitoreo del proveedor Condiciones físicas adversas	Control físico cableado estructurado	50%

Fuente propia

Tabla 25 Vulnerabilidades, controles y nivel de efectividad Cableado Operador

Cableado Operador		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
falta de control de acceso falta monitoreo del proveedor Condiciones físicas adversas	Control físico cableado estructurado	80%

Fuente propia

Tabla 26 Vulnerabilidades, controles y nivel de efectividad Cableado agentes del SIN

Cableado agentes del SIN		
Vulnerabilidades	**Controles actuales implementados en el activo.**	**Efectividad de los controles**
falta de control de acceso falta monitoreo del proveedor Condiciones físicas adversas	Control físico cableado estructurado	50%

Fuente propia

La siguiente matriz tiene el consolidado de los escenarios de riesgos (tabla 27). Un escenario de riesgos en un supuesto de cuando una amenaza puede afectar eventualmente a un activo.

Tabla 27 Cruce de amenazas con activos

ACTIVOS VS AMENAZAS	PMU con S.O comercial	PMU S.O Windows	Roete	Firewall	Switch	Servidores recepción	Personas	Información	Sedes operador	Sedes agentes del SIN	Cableado Operador	Cableado agentes del SIN

Acceso Físico No Autorizado									X	X	X	X
Acceso Lógico No Autorizado	X	X	X	X	X	X		X				
Apt		X				X		X				
Arp Poison					X							
Arp Spoofing					X							
Ataque De Diccionario O Fuerza Bruta	X	X	X	X	X	X						
Ataque DOS Y DDOS	X	X	X	X	X	X						
Ataque Ntp (Desincronización)	X	X	X	X	X	X						
Ataque Sqlinyection		X				X						
Ataque Web	X	X	X	X	X	X						
Código Malicioso		X	X	X	X	X						
Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.)									X	X	X	X
Conflictos personal proyecto							X					
Envenenamiento De XML	X	X	X	X	X	X						
Exploit		X	X	X	X	X						
Ingeniería Social							X					
Interceptación De Cableado											X	X
Daño Cableado Estructurado											X	X
Manipulación De Datos	X	X				X		X				
Obsolescencia Técnica Y Tecnológica	X	X	X	X	X	X			X	X	X	X
Password Craking	X	X	X	X	X	X						
Perdida O Fuga De Información								X				
Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.)									X	X	X	X
Ransomware		X				X						
Rotación O Cambio De Personal Proyecto							X					
Ataque De Direcciones Mac O De Flooding De Mac.			X	X	X							
Scanning	X	X	X	X	X	X						
Suplantación De Identidad	X	X	X	X	X	X	X					
Suplantación De Señales De Control	X	X				X						
XSS	X	X	X	X	X	X						

Fuente propia

4.1.4 Evaluación de riesgos

Se usó la definición de las tablas de probabilidad e impacto, acorde a la metodología para el cálculo de los riesgos, el factor de impacto que se seleccionó es la ***operación***.

Luego se procedió a la calificación de los distintos escenarios, para lo cual, se obtuvieron 139 riesgos, con la siguiente distribución porcentual vista en la figura 8 y en gráfico de tortas en la figura 9

DISTRIBUCIÒN PORCENTUAL

ZONA	%	# Total riesgos
Aceptable	3.31	4
Tolerable	42.98	52
Inaceptable	41.32	50
Inadmisible	12.40	15

Figura 8 Distribución porcentual de riesgos basados en nivel de tolerancia. Fuente propia

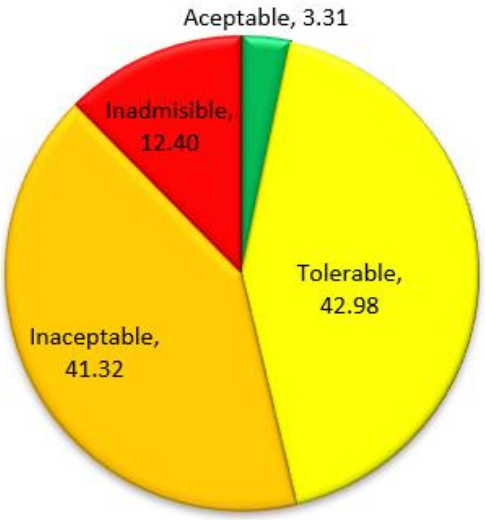


Figura 9: Distribución porcentual de los riesgos encontrados Fuente propia

Como se puede apreciar en la figura 9, se encuentra que un 12,40% de los riesgos son inadmisibles, lo que indica que el proyecto está en alto riesgo y es susceptible a presentarse un ataque informático, los elementos que más preocupan son la falta de controles sobre las PMU prototipo y la falta de hardening sobre la PMU comerciales, algunos de los riesgos inadmisibles están en tabla 28. Riesgos inadmisibles, estos riesgos se deben solucionar en el corto plazo

Los riesgos inaceptables representan un 41,32 % del total de los riesgos (algunos de ellos se indican en Tabla 29), se presentan también en la PMU tanto comerciales como prototipos, adicional se observan activos como servidores e información, también presenta un alto grado de riesgo para el proyecto y se debe definir controles que mitiguen estos riesgos en un mediano plazo.

Para los riesgos tolerables se presenta un 42,98%, estos se pueden trabajar en el largo plazo, a adicionalmente al mitigar los riesgos inadmisibles y los inaceptables es muy probable que bajen el nivel de impacto de muchos de estos.

Adicionalmente solo un 3,31% de los riesgos son aceptables

Tabla 28 Algunos riesgos inadmisibles

No.	Escenario de riesgos inadmisibles	Riesgo P*Impacto
(5)	Posibilidad que la amenaza: Acceso Lógico No Autorizado, afecte el activo: PMU con S.O Comercial	15
(6)	Posibilidad que la amenaza: Acceso Lógico No Autorizado, afecte el activo: PMU S.O Windows	15

(12)	Posibilidad que la amenaza: Apt, afecte el activo: PMU S.O Windows	15
(13)	Posibilidad que la amenaza: Apt, afecte el activo: Servidores recepción	15

Fuente propia

Tabla 29 Algunos Riesgos inaceptables

No.	Escenario de riesgos inaceptables	Riesgo P*Impacto
(1)	Posibilidad que la amenaza: Acceso Físico No Autorizado, afecte el activo: Sedes operador	12
(3)	Posibilidad que la amenaza: Acceso Físico No Autorizado, afecte el activo: Cableado Operador	12
(14)	Posibilidad que la amenaza: Apt, afecte el activo: Información	12
(52)	Posibilidad que la amenaza: Conflictos personal proyecto, afecte el activo: Personas	12

Fuente propia

Nota: En consideración al nivel de confidencialidad de la gestión de riesgos y con el fin de no develar información que pueda ser relevante para el proyecto ISAAC, la mayoría de los riesgos no se presentan, solo se presentan como un compendio global a ser tratados.

4.2 Fase 2: Definición del plan de tratamiento.

4.2.1 Homologación de normas y planes de tratamiento (ISO 27001, NIST CSF y NERC CIP)

La homologación de las normas referenciadas dio como resultados las tabla:

- Tabla 30 Cruce de Normatividad Criterio Identificar del NCF
- Tabla 31 Cruce de Normatividad Criterio proteger de del NCF
- Tabla 32 Cruce de Normatividad Criterio detectar del NCF
- Tabla 33 Cruce de Normatividad Criterio responder del NCF
- Tabla 34 Cruce de Normatividad Criterio recuperar del NCF

Tabla 30 Cruce de Normatividad Criterio Identificar del NCF, controles tomadas de forma textual de las normas respectivas.

IDENTIFICAR			
NIST Cibersecurity Framework 1.1		ISO 27001:2013	Nerc CIP
" Gestión de activos (ID.AM): los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos comerciales y la estrategia de riesgo de la organización."	ID.AM-1: Se inventarean dispositivos y sistemas físicos dentro de la organización"	8.1.1: inventario de activos 8.1.2: propiedad de los activos	CIP-002-5.1a Cyber Security BES Cyber System Categorization R1 CIP-002-5.1a Cyber Security BES Cyber System Categorization R2
	ID.AM-2: se inventarean las plataformas y aplicaciones de software dentro de la organización	8.1.1: inventario de activos 8.1.2: propiedad de los activos	CIP-002-5.1a Cyber Security BES Cyber System Categorization R1 CIP-002-5.1a Cyber Security BES Cyber System Categorization R2
	ID.AM-3: Se asignan los flujos de comunicación y datos de la organización.	13.2.1: políticas y procedimientos de intercambio de información	CIP-003-6 Cyber Security Management Controls R2 y R3
	ID.AM-4: Los sistemas de información externos están catalogados	11.2.6: seguridad de los equipos fuera de las instalaciones	CIP-002-5.1a Cyber Security BES Cyber System Categorization R1 CIP-002-5.1a Cyber Security BES Cyber System Categorization R2
	ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo y software) se priorizan en función de su clasificación, criticidad y valor comercial	8.2.1: clasificación de la información	CIP-002-5.1a Cyber Security BES Cyber System Categorization R1 CIP-002-5.1a Cyber Security BES Cyber System Categorization R2 CIP-005-5 Cyber Security -Electronic Security Perimeter(s)R1
	ID.AM-6: Se establecen roles y responsabilidades de ciberseguridad para toda la fuerza laboral y terceros interesados (por ejemplo, proveedores, clientes, socios)"	6.1.1: roles y responsabilidades en seguridad de la información	CIP-003-6 Cyber Security Management Controls R3 CIP-003-6 Cyber Security Management Controls R4
Entorno empresarial (ID.BE): la misión, los objetivos, las partes interesadas y las actividades de la organización se entienden y priorizan; Esta información se utiliza para informar las	ID.BE-1: Se identifica y se comunica el papel de la organización en la cadena de suministro.	15.1.3: cadena de suministro de tecnología de la información y de las comunicaciones 15.2.1: control y revisión de la provisión de servicios del proveedor 15.2.2: gestión de cambios en la provisión del servicio del proveedor	CIP-013-1 -Cyber Security - Supply Chain Risk Management R1
	ID.BE-2: Se identifica y comunica el lugar de la organización en la infraestructura crítica y su sector industrial."	6.1.3 contacto con las autoridades. 6.1.4 contacto con grupos de interés especial.	

funciones de seguridad cibernética, las responsabilidades y las decisiones de gestión de riesgos.	ID.BE-3: Se establecen y comunican las prioridades para la misión, los objetivos y las actividades de la organización.		
	ID.BE-4: Se establecen dependencias y funciones críticas para la prestación de servicios críticos.	11.2.2: instalaciones de suministros 11.2.3: seguridad del cableado 12.1.3: gestión de capacidades	CIP-003-6 Cyber Security Management Controls R1 R2 CIP-013-1 -Cyber Security - Supply Chain Risk Management R!
	ID.BE-5: Se establecen requisitos de resistencia para respaldar la prestación de servicios críticos para todos los estados operativos (por ejemplo, bajo coacción / ataque, durante la recuperación, operaciones normales)	11.1.4: protección contra las amenazas externas y ambientales 17.1.1: planificación de la continuidad de la seguridad de la información 17.1.2: implementar la continuidad de la seguridad de la información 17.2.1: disponibilidad de los recursos de tratamiento de la información	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
Gobernanza (ID. GV): las políticas, procedimientos y procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se entienden e informan a la administración del riesgo de ciberseguridad.	ID. GV-1: se establece la política de seguridad de la información organizacional	5.1.1: políticas para la seguridad de la información	CIP-003-6 Cyber Security Management Controls R1 CIP-003-6 Cyber Security Management Controls R2
	ID. GV-2: Las funciones y responsabilidades de seguridad de la información están coordinadas y alineadas con las funciones internas y los socios externos."	6.1.1: roles y responsabilidades en seguridad de la información 7.2.1. responsabilidades de gestión	CIP-003-6 Cyber Security Management Controls R1 CIP-003-6 Cyber Security Management Controls R2
	ID. GV-3: Los requisitos legales y reglamentarios con respecto a la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles, se entienden y gestionan	18.1.1. identificación de la legislación aplicable y d ellos requisitos contractuales	
	ID. GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad	6.1.1 asignación de responsabilidades para la segur. de la información. 6.1.2 segregación de tareas.	CIP-003-6 Cyber Security Management Controls R2 y R3
Evaluación de riesgos (ID.RA): la organización comprende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, funciones, imagen o reputación), los activos de la organización y las personas.	ID.RA-1: las vulnerabilidades de los activos se identifican y documentan	12.6.1: gestión de las vulnerabilidades técnicas 18.2.3: comprobación del cumplimiento técnico	CIP-007-6 Cyber Security -Systems Security Management R2 CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R3
	ID.RA-2: se recibe información de inteligencia y vulnerabilidad sobre amenazas cibernéticas de fuentes y foros de intercambio de información	6.1.4: contacto con grupos de interés de interés especial 6.1.3 contacto con las autoridades.	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability
	ID.RA-3: las amenazas, tanto internas como externas, se identifican y documentan	16.1.1 responsabilidades y procedimientos.	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability

		16.1.2 notificación de los eventos de seguridad de la información. 16.1.3 notificación de puntos débiles de la seguridad. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	
	ID.RA-4: Se identifican los posibles impactos en el negocio y las probabilidades	16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-004-6 Cyber Security -Personnel & Training R3 CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	ID.RA-5: las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo	12.6.1: gestión de las vulnerabilidades técnicas	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R3
	ID.RA-6: Las respuestas al riesgo se identifican y priorizan"	16.1.1 responsabilidades y procedimientos. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-004-6 Cyber Security -Personnel & Training R3
" Estrategia de gestión de riesgos (ID.RM): las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para respaldar las decisiones de riesgo operativo."	ID.RM-1: los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización	16.1.1 responsabilidades y procedimientos. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-004-6 Cyber Security -Personnel & Training R3 CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	ID.RM-2: la tolerancia al riesgo organizacional se determina y se expresa claramente"	16.1.1 responsabilidades y procedimientos. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-004-6 Cyber Security -Personnel & Training R3 CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	ID.RM-3: La determinación de la organización de la tolerancia al riesgo se basa en su papel en la infraestructura crítica y el análisis de riesgos específicos del sector."	16.1.1 responsabilidades y procedimientos. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-004-6 Cyber Security -Personnel & Training R3 CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	ID.SC-1: los procesos de gestión de riesgos de la cadena de suministro cibernética son identificados, establecidos, evaluados,	15.1.1: política de seguridad de la información en las relaciones con los proveedores	CIP-013-1 -Cyber Security - Supply Chain Risk Management R2

Gestión de riesgos de la cadena de suministro (ID.SC): las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización cuenta con procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	gestionados y acordados por las partes interesadas de la organización	15.1.2: requisitos de seguridad en contratos con terceros 15.1.3: cadena de suministro de tecnología de la información y de las comunicaciones 15.2.1: control y revisión de la provisión de servicios del proveedor 15.2.2: gestión de cambios en la provisión del servicio del proveedor	
	ID.SC-2: Identificar, priorizar y evaluar proveedores y socios de sistemas, componentes y servicios de información crítica utilizando un proceso de evaluación de riesgos de la cadena de suministro cibernético"	15.2.1: control y revisión de la provisión de servicios del proveedor 15.2.2: gestión de cambios en la provisión del servicio del proveedor	CIP-013-1 -Cyber Security - Supply Chain Risk Management R2
	ID.SC-3: Los proveedores y socios deben, por contrato, implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de Seguridad de la Información o el Plan de Gestión de Riesgos de la Cadena de Suministro Cibernético."	15.1.1: política de seguridad de la información en las relaciones con los proveedores 15.1.2: requisitos de seguridad en contratos con terceros 15.1.3: cadena de suministro de tecnología de la información y de las comunicaciones	CIP-013-1 -Cyber Security - Supply Chain Risk Management R2
	ID.SC-4: Los proveedores y socios son monitoreados para confirmar que han cumplido con sus obligaciones según lo requerido. Se llevan a cabo revisiones de auditorías, resúmenes de resultados de pruebas u otras evaluaciones equivalentes de proveedores / proveedores.	15.2.1: control y revisión de la provisión de servicios del proveedor 15.2.2: gestión de cambios en la provisión del servicio del proveedor	CIP-013-1 -Cyber Security - Supply Chain Risk Management R2
	ID.SC-5: La planificación y las pruebas de respuesta y recuperación se realizan con proveedores / proveedores críticos"	17.1.3: verificación, revisión y evaluación de la continuidad de la seguridad de la información	CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1

Fuente propia a partir de las normas

Tabla 31 Cruce de Normatividad Criterio proteger de del NCF, definiciones tomadas de forma textual de las normas.

PROTEGER			
NIST Cibersecurity Framework 1.1		ISO 27001:2013	Nerc CIP
Gestión de identidad y control de acceso (PR.AC): el acceso a los activos físicos y lógicos y las instalaciones asociadas está limitado a usuarios, procesos y dispositivos autorizados, y se gestiona de forma coherente con el riesgo evaluado de acceso no autorizado.	PR.AC-1: las identidades y credenciales se emiten, administran, revocan y auditan para dispositivos, usuarios y procesos autorizados	9.2.1: registro y baja de usuario 9.2.2: provisión de acceso de usuario 9.2.4: gestión de la información secreta de autenticación de los usuarios 9.3.1: uso de la información secreta de autenticación 9.4.2: procedimientos seguros de inicio de sesión 9.4.3: sistema de gestión de contraseñas	CIP-004-6 Cyber Security –Personnel & Training R4 CIP-004-6 Cyber Security –Personnel & Training R5 CIP-007-6 Cyber Security -Systems Security Management R4 R5
	PR.AC-2: el acceso físico a los activos se gestiona y protege"	11.1.1: perímetro de seguridad física 11.1.2. controles físicos de entrada 11.1.4: protección contra las amenazas externas y ambientales 11.1.6: áreas de carga y descarga 11.2.3: seguridad del cableado	CIP-004-6 Cyber Security –Personnel & Training R4 CIP-004-6 Cyber Security –Personnel & Training R5 CIP-006-6 Cyber Security Physical Security of BES Cyber Systems r1 y R2
	PR.AC-3: se administra el acceso remoto"	6.2.2: teletrabajo 13.1.1: controles de red 13.2.1: políticas y procedimientos de intercambio de información	CIP-004-6 Cyber Security Personnel & Training R5 CIP-005-5 Cyber Security –Electronic Security Perimeter(s)R2 CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-013-1 -Cyber Security - Supply Chain Risk Management r1
	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso, incorporando los principios de menor privilegio y separación de funciones."	6.1.2: segregación de tareas 9.1.2: acceso a las redes y a los servicios de red 9.2.3: gestión de privilegios de acceso 9.4.1: restricción del acceso a la información 9.4.4: uso de utilidades con privilegios del sistema	CIP-004-6 Cyber Security –Personnel & Training R4 CIP-004-6 Cyber Security –Personnel & Training R5 CIP-006-6 Cyber Security Physical Security of BES Cyber Systems r1 y R2 CIP-007-6 Cyber Security -Systems Security Management R4 R5
	PR.AC-5: La integridad de la red está protegida, incorporando segregación de red cuando sea apropiado"	13.1.1: controles de red 13.1.3: segregación en redes 13.2.1: políticas y procedimientos de intercambio de información	CIP-005-5 Cyber Security -Electronic Security Perimeter(s)R1 CIP-007-6 Cyber Security -Systems Security Management R4 R5
	PR.AC-6: las identidades se prueban y se unen a las credenciales, y se afirman en las interacciones cuando corresponde	6.1.2: segregación de tareas 7.1.1: investigación de antecedentes 9.1.2: acceso a las redes y a los usuarios de red 9.2.2: provisión de acceso de usuario	CIP-004-6 Cyber Security –Personnel & Training R4 CIP-004-6 Cyber Security -Personnel & Training R5 CIP-007-6 Cyber Security -Systems Security Management R4 R5

		9.2.3: gestión de privilegios de acceso 9.2.5: revisión de los derechos de acceso de usuario 9.2.6: retirada o reasignación de los derechos de acceso 9.4.1: restricción del acceso a la información 9.4.4: uso de utilidades con privilegios del sistema	
Conciencia y capacitación (PR.AT): el personal y los socios de la organización reciben educación sobre concientización en seguridad cibernética y están capacitados adecuadamente para realizar sus deberes y responsabilidades relacionados con la seguridad de la información de acuerdo con las políticas, procedimientos y acuerdos relacionados	PR.AT-1: Todos los usuarios están informados y capacitados."	7.2.2: conciencia, educación y capacitación en seguridad de la información	CIP-004-6 Cyber Security -personnel & Training R1 CIP-004-6 Cyber Security –Personnel & Training R2
	PR.AT-2: los usuarios privilegiados comprenden roles y responsabilidades"	6.1.1: roles y responsabilidades en seguridad de la información 7.2.2: conciencia, educación y capacitación en seguridad de la información	CIP-004-6 Cyber Security -personnel & Training R1 CIP-004-6 Cyber Security –Personnel & Training R2
	PR.AT-3: las partes interesadas de terceros (p. Ej., Proveedores, clientes, socios) comprenden los roles y las responsabilidades"	6.1.1: roles y responsabilidades en seguridad de la información 7.2.2: conciencia, educación y capacitación en seguridad de la información	CIP-004-6 Cyber Security -personnel & Training R1 CIP-004-6 Cyber Security –Personnel & Training R2
	PR.AT-4: altos ejecutivos entienden roles y responsabilidades	6.1.1: roles y responsabilidades en seguridad de la información 7.2.2: concientización, educación y capacitación en seguridad de la información	CIP-004-6 Cyber Security -personnel & Training R1 CIP-004-6 Cyber Security –Personnel & Training R2
	PR.AT-5: El personal de seguridad física y de información comprende los roles y responsabilidades"	6.1.1: roles y responsabilidades en seguridad de la información 7.2.2: concientización, educación y capacitación en seguridad de la información	CIP-004-6 Cyber Security -personnel & Training R1 CIP-004-6 Cyber Security –Personnel & Training R2
Seguridad de datos (PR.DS): la información y los registros (datos) se administran de manera coherente con la estrategia de riesgos de la organización para proteger la confidencialidad,	PR.DS-1: los datos en reposo están protegidos+	8.2.3: clasificación de la información	CIP-011-2 Cyber Security Information Protection R1
	PR.DS-2: los datos en tránsito están protegidos"	8.2.3: manipulado de la información 13.1.1: controles de red 13.2.1: políticas y procedimientos de intercambio de información 13.2.3: mensajería electrónica 14.1.2: asegurar los servicios de aplicaciones en redes publicas 14.1.3: protección de las transacciones de servicios de aplicaciones	CIP-011-2 Cyber Security Information Protection R1
	PR.DS-3: los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición	8.2.3: manipulado de la información 8.3.1: gestión de soportes extraíbles 8.3.2: eliminación de soportes 8.3.3: soportes físicos en transito 11.2.7: reutilización o eliminación segura de equipos	CIP-011-2 Cyber Security Information Protection R1

integridad y disponibilidad de la información.	PR.DS-4: capacidad adecuada para garantizar que se mantenga la disponibilidad"	12.3.1: copias de seguridad de la información	CIP-004-6 Cyber Security -Personnel & Training R2 CIP-003-6 Cyber Security Management Controls R3 y R4
	PR.DS-5: se implementan protecciones contra fugas de datos	6.1.2: segregación de tareas 7.1.1: investigación de antecedentes 7.1.2: términos y condiciones del empleo 7.3.1: responsabilidades ante la finalización o cambio 8.2.2: etiquetado de la información 8.2.3: manipulado de la información 9.1.1: política de control de acceso 9.1.2: acceso a las redes y a los servicios de red 9.2.3: gestión de privilegios de acceso 9.4.1: restricción del acceso a la información 9.4.4: uso de utilidades de privilegios del sistema 9.4.5: control de acceso al código fuente de los programas 13.1.3: segregación en redes 13.2.1: políticas y procedimientos de intercambio de información 13.2.3: mensajería electrónica 13.2.4: acuerdos de confidencialidad o no renovación 14.1.2: asegurar los servicios de aplicaciones en redes publicas 14.1.3: protección de las transacciones de servicios de aplicaciones	CIP-011-2 Cyber Security Information Protection R1
	PR.DS-6: los mecanismos de verificación de integridad se utilizan para verificar el software, el firmware y la integridad de la información"	12.2.1: controles contra el código malicioso 12.5.1: instalación del software en explotación 14.1.2: asegurar los servicios de aplicaciones en redes publicas 14.1.3: protección de las transacciones de servicios de aplicaciones	CIP-007-6 Cyber Security -Systems Security Management R3
	PR.DS-7: los entornos de desarrollo y prueba están separados del entorno de producción"	12.1.4: separación de los recursos de desarrollo, prueba y operación	
	PR.DS-8: los mecanismos de verificación de integridad se utilizan para verificar la integridad del hardware"	11.2.4: mantenimiento de los equipos	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R1 y R2

Procesos y procedimientos de protección de la información (PIPI): las políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de gestión y la coordinación entre las entidades de la organización), los procesos y procedimientos se mantienen y utilizan para gestionar la protección de los sistemas y activos de información.	"PR. IP-1: se crea y mantiene una configuración de línea base de tecnología de la información / sistemas de control industrial que incorpora principios de seguridad apropiados (por ejemplo, el concepto de menor funcionalidad)	12.1.2: gestión de cambios 12.5.1: instalación del software en explotación 12.6.2: restricción en la instalación de software 14.2.2: procedimiento de control de cambios en sistemas 14.2.3: revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 14.2.4: restricciones a los cambios en los paquetes de software	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R1
	PR. IP-2: se implementa un ciclo de vida de desarrollo de sistemas para administrar sistemas"	6.1.5: seguridad de la información en la gestión de proyectos 14.1.1: análisis de requisitos y especificaciones de seguridad de la información 14.2.1: política de desarrollo seguro 14.2.5: principios de ingeniería de sistemas seguros	CIP-013-1 -Cyber Security - Supply Chain Risk Management
	PR. IP-3: los procesos de control de cambio de configuración están en su lugar	12.1.2: gestión de cambios 12.5.1: instalación del software en explotación 12.6.2: restricción en la instalación de software 14.2.2: procedimiento de control de cambios en sistemas 14.2.3: revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 14.2.4: restricciones a los cambios en los paquetes de software	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability
	PR. IP-4: las copias de seguridad de la información se realizan, mantienen y prueban periódicamente"	12.3.1: copias de seguridad de la información 17.1.2: implementar la continuidad de la seguridad de la información 17.1.3: verificación, revisión y evaluación de la continuidad de la seguridad de la información 18.1.3: protección de los registros de la organización	CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R2 y R3
	PR. IP-5: Se cumplen las políticas y regulaciones sobre el entorno operativo físico para los activos de la organización."	11.1.4: protección contra las amenazas externas y ambientales a 11.2.1: emplazamiento y protección de equipos · 11.2.2: instalaciones de suministro 11.2.3: seguridad del cableado	CIP-006-6 Cyber Security Physical Security of BES Cyber Systems r1 y R2
	PR. IP-6: los datos se destruyen de acuerdo con la política"	8.2.3: manipulado de la información 8.3.1: gestión de soportes extraíbles 8.3.2: eliminación de soportes 11.2.7: reutilización o eliminación segura de equipos	CIP-011-2 Cyber Security Information Protection r2

	PR. IP-7: los procesos de protección se mejoran continuamente"	12.1.1 documentación de procedimientos de operación. 12.1.2 gestión de cambios. 12.1.3 gestión de capacidades.	CIP-011-2 Cyber Security Information Protection r1
	PR. IP-8: la eficacia de las tecnologías de protección se comparte con las partes apropiadas"	16.1.6: aprendizaje de los incidentes de seguridad de la información	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1
	PR. IP-9: Planes de respuesta (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres) implementados y administrados	16.1.1: responsabilidades y procedimientos 17.1.1: planificación de la continuidad de la seguridad de la información 17.1.2: implementar la continuidad de la seguridad de la información	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	PR. IP-10: se prueban los planes de respuesta y recuperación	17.1.3: verificación, revisión y evaluación de la continuidad de la seguridad de la información	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
	PR. IP-11: La ciberseguridad está incluida en las prácticas de recursos humanos (por ejemplo, des aprovisionamiento, selección de personal)	7.1.1: investigación de antecedentes 7.3.1: responsabilidades ante la finalización o cambio 8.1.4: devolución de activos	CIP-004-6 Cyber Security -Personnel & Training R3
	PR. IP-12: se desarrolla e implementa un plan de gestión de vulnerabilidades	12.6.1: gestión de las vulnerabilidades técnicas 18.2.2: cumplimiento de la políticas y normas de seguridad	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R1 CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R3
" Mantenimiento (PR.MA): el mantenimiento y las reparaciones de los componentes del control industrial y del sistema de información se realizan de acuerdo con las políticas y procedimientos."	PR.MA-1: El mantenimiento y reparación de los activos de la organización se realiza y registra de manera oportuna, con herramientas aprobadas y controladas.	11.1.2: controles físicos de entrada 11.2.4: mantenimiento de los equipos 11.2.5: retirada de materiales propiedad de la empresa	CIP-006-6 Cyber Security Physical Security of BES Cyber Systems R3
	PR.MA-2: el mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de una manera que impide el acceso no autorizado	11.2.4: mantenimiento de los equipos 15.1.1: política de seguridad de la información en las relaciones con los proveedores 15.2.1: control y revisión de la provisión de servicios del proveedor	CIP-005-5 Cyber Security -Electronic Security Peri meter(s)R2 CIP-013-1 -Cyber Security - Supply Chain Risk Management R1
	PR.PT-1: los registros de auditoría / registro se determinan, documentan, implementan y revisan de acuerdo con la política	12.4.1: registro de eventos 12.4.2: protección de la información del registro 12.4.3: registros de administración y operación 12.4.4: sincronización del reloj	CIP-007-6 Cyber Security -Systems Security Management R4 R5

Tecnología de protección (PR.PT): las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resistencia de los sistemas y activos, de conformidad con las políticas, procedimientos y acuerdos relacionados.		12.7.1: controles de auditoria de sistemas de información	
	PR.PT-2: los medios extraíbles están protegidos y su uso está restringido de acuerdo con la política	8.2.2: etiquetado de la información 8.2.3: manipulado de la información 8.3.1: gestión de soportes extraíbles 8.3.3: soportes físicos en transito 11.2.9: política de puesto de trabajo despejado y pantalla limpia	CIP-007-6 Cyber Security -Systems Security Management R1 CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R4
	PR.PT-3: el principio de menor funcionalidad se incorpora mediante la configuración de sistemas para proporcionar solo capacidades esenciales	9.1.2: acceso a las redes y a los servicios de red	CIP-007-6 Cyber Security -Systems Security Management R1
	PR.PT-4: las redes de comunicaciones y control están protegidas	13.1.1: controles de red 13.2.1: políticas y procedimientos de intercambio de información	CIP-007-6 Cyber Security -Systems Security Management R1
	PR.PT-5: Los sistemas operan en estados funcionales predefinidos para lograr disponibilidad (por ejemplo, bajo coacción, bajo ataque, durante la recuperación, operaciones normales).	17.1.2: implementar la continuidad de la seguridad de la información 17.2.1: disponibilidad de los recursos de tratamiento de la información	CIP-007-6 Cyber Security -Systems Security Management R1

Fuente propia a partir de las normas

Tabla 32 Cruce de Normatividad Criterio detectar del NCF

DETECTAR			
NIST Cibersecurity Framework 1.1		ISO 27001:2013	Nerc CIP
Anomalías y eventos (DE.AE): la actividad	DE.AE-1: se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas	12.1.1 documentación de procedimientos de operación. 12.1.2 gestión de cambios. 12.1.3 gestión de capacidades. 12.1.4 separación de entornos de desarrollo, prueba y producción.	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability CIP-007-6 Cyber Security -Systems Security Management R1
	DE.AE-2: los eventos detectados se analizan para comprender los objetivos y métodos de ataque	16.1.1: responsabilidades y procedimientos 16.1.4: evaluación y decisión sobre los eventos de seguridad de información	CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R1

anómala se detecta de manera oportuna y se entiende el impacto potencial de los eventos.	DE.AE-3: los datos de eventos se agregan y se correlacionan desde múltiples fuentes y sensores	16.1.1 responsabilidades y procedimientos. 16.1.5 respuesta a los incidentes de seguridad.	CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	DE.AE-4: Se determina el impacto de los eventos.	16.1.1 responsabilidades y procedimientos. 16.1.4 valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 respuesta a los incidentes de seguridad.	CIP-007-6 Cyber Security -Systems Security Management R4 CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	DE.AE-5: se establecen umbrales de alerta de incidentes	16.1.1 responsabilidades y procedimientos. 16.1.5 respuesta a los incidentes de seguridad.	CIP-007-6 Cyber Security -Systems Security Management R4
Monitoreo continuo de seguridad (DE.CM): el sistema de información y los activos se monitorean a intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	DE.CM-1: la red se supervisa para detectar posibles eventos de ciberseguridad	12.4.1 registro y gestión de eventos de actividad. 12.4.2 protección de los registros de información. 12.4.3 registros de actividad del administrador y operador del sistema 12.7.1 controles de auditoría de los sistemas de información.	CIP-007-6 Cyber Security -Systems Security Management R4
	DE.CM-2: el entorno físico se controla para detectar posibles eventos de ciberseguridad"	11.1.2 controles físicos de entrad 11.1.3 seguridad de oficinas, despachos y recursos. 11.1.4 protección contra las amenazas externas y ambientales. 11.1.5 el trabajo en áreas seguras. 11.1.6 áreas de acceso público, carga y descarga	CIP-006-6 Cyber Security Physical Security of BES Cyber Systems r1
	DE.CM-3: se supervisa la actividad del personal para detectar posibles eventos de ciberseguridad"	12.4.1: registro de eventos	CIP-007-6 Cyber Security -Systems Security Management R4 R5
	DE.CM-4: se detecta código malicioso"	12.2.1: controles contra el código malicioso	CIP-007-6 Cyber Security -Systems Security Management R3
	DE.CM-5: se detecta un código móvil no autorizado"	12.5.1: instalación del software en explotación	CIP-007-6 Cyber Security -Systems Security Management R3
	DE.CM-6: se supervisa la actividad del proveedor de servicios externos para detectar posibles eventos de ciberseguridad"	14.2.7: externalización del desarrollo de software	CIP-007-6 Cyber Security -Systems Security Management R4 R5

		15.2.1: control y revisión de la provisión de servicios del proveedor	
	DE.CM-7: Monito ring for unauthorized personnel, connections, devices, and software is performed	12.4.1 registro y gestión de eventos de actividad. 12.4.2 protección de los registros de información. 12.4.3 registros de actividad del administrador y operador del sistema 12.7.1 controles de auditoría de los sistemas de información.	CIP-007-6 Cyber Security -Systems Security Management R4 R5
	DE.CM-8: se realizan exploraciones de vulnerabilidad"	12.6.1: gestión de las vulnerabilidades técnicas	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability r3
Procesos de detección (DEDO): los procesos y procedimientos de detección se mantienen y prueban para garantizar el conocimiento oportuno y adecuado de eventos anómalos.	DE. DP-1: los roles y las responsabilidades para la detección están bien definidos para garantizar la responsabilidad"	6.1.1: roles y responsabilidades en seguridad de la información	CIP-003-6 Cyber Security Management Controls R3 CIP-003-6 Cyber Security Management Controls R4 CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	DE. DP-2: las actividades de detección cumplen con todos los requisitos aplicables	18.1.4: protección y privacidad de la información de carácter personal	CIP-007-6 Cyber Security -Systems Security Management R4 R5
	DE. DP-3: se prueban los procesos de detección"	14.2.8: pruebas funcionales de seguridad de sistemas	CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R2
	DE. DP-4: la información de detección de eventos se comunica a las partes correspondientes"	16.1.2: notificación de los eventos de seguridad de la información	CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R2
	DE. DP-5: los procesos de detección se mejoran continuamente	16.1.6: aprendizaje de los incidentes de seguridad de la información	CIP-007-6 Cyber Security -Systems Security Management R4 5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R2

Tabla 33 Cruce de Normatividad Criterio responder del NCF. Definiciones tomadas de forma textual de las normas.

RESPONDER			
NIST Cibersecurity Framework 1.1		ISO 27001:2013	Nerc CIP
"Planificación de respuesta (RS.RP): los procesos y procedimientos de respuesta se ejecutan y mantienen para garantizar una respuesta oportuna a los eventos de ciberseguridad detectados.	RS.RP-1: el plan de respuesta se ejecuta durante o después de un evento	16.1.5: respuesta a incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R2
Comunicaciones (RS.CO): las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda, para incluir el apoyo externo de las agencias de aplicación de la ley.	RS.CO-1: el personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta	6.1.1: roles y responsabilidades en seguridad de la información 16.1.1: responsabilidades y procedimientos	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	RS.CO-2: los eventos se informan de acuerdo con los criterios establecidos	6.1.3: contacto con las autoridades 16.1.2: notificación de los eventos de seguridad de la información	CIP-007-6 Cyber Security -Systems Security Management R4 R5 CIP-008-5 Cyber Security Incident Reporting and Response Planning R2
	RS.CO-3: la información se comparte de acuerdo con los planes de respuesta	16.1.2: notificación de los eventos de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R2
	RS.CO-4: La coordinación con las partes interesadas ocurre de acuerdo con los planes de respuesta"	16.1.2 notificación de los eventos de seguridad de la información. 16.1.5 respuesta a los incidentes de seguridad.	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	RS.CO-5: El intercambio voluntario de información se produce con partes interesadas externas para lograr una mayor conciencia de la situación de ciberseguridad	16.1.2 notificación de los eventos de seguridad de la información. 16.1.3 notificación de puntos débiles de la seguridad.	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
Análisis (RS.AN): el análisis se realiza para garantizar una respuesta adecuada y apoyar	RS.AN-1: se investigan las notificaciones de los sistemas de detección	12.4.1: registro de eventos 12.4.3: registros de administración y operación 16.1.5: respuesta a incidentes de seguridad de la información	CIP-007-6 Cyber Security -Systems Security Management R4 r5
	RS.AN-2: se entiende el impacto del incidente	16.1.6: aprendizaje de los incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1

las actividades de recuperación.	RS.AN-3: se realizan análisis forenses	16.1.7: recopilación de evidencias	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	RS.AN-4: los incidentes se clasifican de acuerdo con los planes de respuesta"	16.1.4: evaluación y decisión sobre los eventos de seguridad de información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
Mitigación (RS.MI): se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y erradicar el incidente.	RS.MI-1: los incidentes están contenidos	16.1.5: respuesta a incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	RS.MI-2: los incidentes se mitigan	12.2.1: controles contra el código malicioso 16.1.5: respuesta a incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
	RS.MI-3: las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados	12.6.1: gestión de las vulnerabilidades técnicas	CIP-010-2 Cyber Security Configuration Change Management and Vulnerability R3 CIP-008-5 Cyber Security Incident Reporting and Response Planning R1
Mejoras (RS.IM): las actividades de respuesta organizacional se mejoran al incorporar las lecciones aprendidas de las actividades de detección / respuesta actuales y anteriores.	RS.IM-1: los planes de respuesta incorporan las lecciones aprendidas"	16.1.6: aprendizaje de los incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R3
	RS.IM-2: las estrategias de respuesta se actualizan	16.1.6: aprendizaje de los incidentes de seguridad de la información	CIP-008-5 Cyber Security Incident Reporting and Response Planning R3

Fuente propia a partir de las normas

Tabla 34 Cruce de Normatividad Criterio recuperar del NCF. Definiciones tomadas de forma textual de las normas

RECUPERAR			
NIST Cibersecurity Framework 1.1		ISO 27001:2013	Nerc CIP
Planificación de recuperación (RC.RP): los procesos y procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.	" RC.RP-1: el plan de recuperación se ejecuta durante o después de un evento"	16.1.5: respuesta a incidentes de seguridad de la información a17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información.	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1
Mejoras (RC.IM): la planificación y los procesos de recuperación se mejoran al incorporar las lecciones aprendidas en actividades futuras.	RC.IM-1: los planes de recuperación incorporan las lecciones aprendidas	a17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información.	CIP-009-5 Cyber Security Incident Reporting and Response Planning R3 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems r2 y R3
	RC.IM-2: se actualizan las estrategias de recuperación"	a17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información.	CIP-009-5 Cyber Security Incident Reporting and Response Planning R3 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R3
Comunicaciones (RC.CO): las actividades de restauración se coordinan con partes internas y externas, como centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y proveedores.	RC.CO-1: se gestionan las relaciones públicas"		
	RC.CO-2: Reputación después de que se repara un evento"	16.1.5: respuesta a incidentes de seguridad de la información a17.1.3 verificación, revisión y evaluación de la continuidad de la seguridad de la información.	CIP-009-5 Cyber Security Incident Reporting and Response Planning R3 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R3
	RC.CO-3: las actividades de recuperación se comunican a las partes interesadas internas y a los equipos ejecutivos y de gestión	a 17.1.1 planificación de la continuidad de la seguridad de la información. a17.1.2 implantación de la continuidad de la seguridad de la información.	CIP-009-5 Cyber Security Incident Reporting and Response Planning R1 CIP-009-6 Cyber Security Recovery Plans for BES Cyber Systems R1

Fuente propia a partir de las normas

4.2.2 Planes de tratamiento

A continuación, se describe el detalle de cada uno de los planes de tratamiento ver tablas (tabla 35 - tabla 53), las cuales se definieron para mitigas los riesgos inaceptables e inadmisibles.

Tabla 35 Plan Segmentación de red

Segmentación de red	
Descripción	Se debe generar un modelo de segmentación de red que permita separar los equipos de pruebas de productivos, adicionalmente se deben corregir los errores de direccionamiento existentes, así como ajuste os servidores que tienen doble tarjeta de red
Activos afectados	servidores, PMU comerciales, PMU prototipo, firewall, router.
Riesgos / amenazas mitigadas	Acceso Lógico No Autorizado, Arp Poison, Ataque De Diccionario O Fuerza Bruta, Ataque Ntp (Desincronización), Ataque Web, Código Malicioso, Envenenamiento De XML, Exploit, Ataque DOS Y DDOS, Obsolescencia Técnica Y Tecnológica, Suplantación De Identidad, Password Craking, Ransomware,
tecnología a implementar	Router y Firewall

Fuente propia

Tabla 36 Plan Cambio de sistema operativo obsoleto

Cambio de sistema operativo por obsolescencia	
Descripción	Realizar cambio de sistema operativo sobre las PMU prototipo que tienen sistema operativo Windows
Activos afectados	PMU tipo prototipo
Riesgos /amenazas a mitigadar	Acceso Lógico No Autorizado, Apt, Ataque De Diccionario O Fuerza Bruta, Ataque NTP Código Malicioso, (Desincronización), Exploit, Suplantación De Identidad, Suplantación De Señales De Control
tecnología a implementar	implementación sistema operativo en sus últimas versiones o la que sea soportada.

Fuente propia

Tabla 37 Plan línea base para las PMU comerciales

línea base para las PMU comerciales	
Descripción	Definir la línea base para las PMU comerciales que permita mitigar los riesgos asociados a estas, las cuales comprenden: Cambios de contraseña por defectos Ajuste en puertos y servicios inseguros y utilizados Segregación de roles Reporte de log
Activos afectados	PMU Comerciales
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Web, Obsolescencia Técnica Y Tecnológica, Suplantación De Identidad, Suplantación De Señales De Control, Manipulación De Datos, Ataque Ntp (Desincronización).
tecnología a implementar	N/A

Tabla 38 Plan Controlador de domino

Controlador de domino	
Descripción	Implementación de controlador de domino ubicado en el segmento de servidores, y configuración de políticas de dominio para unidad organizacional nueva, esto con el fin de controlar los equipos tipo Windows servidores y PMU tipo prototipo
Activos afectados	equipos con sistema operativo Windows y servidores Windows
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Apt, Ataque De Diccionario O Fuerza Bruta, Código Malicioso, Ransomware, Ataque DOS Y DDOS, Exploit, Scanning, Suplantación De Señales De Control,
tecnología a implementar	Windows server controlador dominio con unidad organizacional y políticas específicas para la red

Fuente propia

Tabla 39 Plan monitoreo por el SOC

Monitoreo por el SOC	
Descripción	Implementación de monitoreo sobre los distintos componentes tecnológicos de la red, sea mediante la instalación de agentes, syslog o por medio de monitoreo de trafico de red
Activos afectados	Todos los activos tecnológicos: PMU prototipo, PMU comerciales, servidores, equipos de red y equipos firewall, información
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Arp Poison, Ataque De Diccionario O Fuerza Bruta, Ataque Web, : Exploit, Ataque Ntp (Desincronización), Password Craking, Ataque DOS Y DDOS, Apt, Código Malicioso, Manipulación De Datos, Saturación De Direcciones Mac O Ataques De Flooding De Mac., Ataque Ntp (Desincronización)
tecnología a implementar	Correlacionado de eventos alienvault, colector de log greylog, instalación de agentes ossec en máquinas Windows, puerto espejo de red (NIDS)

Fuente propia

Tabla 40 Plan Actualizaciones de firmware

Actualizaciones de firmware	
Descripción	Actualizar el firmware de las PMU comerciales y los equipos de comunicaciones y firewall a la última versión estable, así como
Activos afectados	PMU comerciales, SW, firewall
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Arp Poison, Arp Spoofing, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización), Ataque Web, Código Malicioso, Envenenamiento De XML, Exploit, Obsolescencia Técnica Y Tecnológica, Password Craking, Saturación De Direcciones Mac O Ataques De Flooding De Mac., Scanning, Suplantación De Identidad, XSS
tecnología a implementar	Firmware de PMU comercial, SW y firewall

Fuente propia

Tabla 41 Plan servicio de ciber inteligencia del SOC

servicio de ciber inteligencia del SOC, convenio de cooperación con CCOCI o COLCERT, Participación en grupos sectoriales de seguridad y del ministerio	
Descripción	Incorporar los activos de la red ISAAC en los sistemas de monitoreo y de ciber inteligencia de la organización
Activos afectados	Todos los activos de la red ISAAC
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Acceso Lógico No Autorizado, Apt, Arp Poison, Arp Spoofing, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización), Ataque Sqlinyection, Ataque Web, Código Malicioso, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Conflictos personal proyecto, Envenenamiento De XML, Exploit, Ingeniería Social, Interceptación De Cableado, Daño Cableado Estructurado, Manipulación De Dato, Obsolescencia Técnica Y Tecnológica, Password Craking, Perdida O Fuga De Información, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), Ransomware, Rotación O Cambio De Personal Gestor Del Proyecto, Saturación De Direcciones Mac O Ataques De Flooding De Mac, Scanning, Suplantación De Identidad, Suplantación De Señales De Control
tecnología a implementar	plataforma de ciber inteligencia, intercambio información

Fuente propia

Tabla 42 Plan Procedimiento para análisis de vulnerabilidades

Procedimiento para análisis de vulnerabilidades periódico (trimestral) y planes de remediación	
Descripción	Programar análisis de vulnerabilidades trimestrales sobre dispositivos, realizar plan de mitigación.
Activos afectados	Todos los equipos tecnológicos y toda la red
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Arp Poison, Ataque De Diccionario O Fuerza Bruta, Ataque Web, : Exploit, Ataque Ntp (Desincronización), Password Craking, Ataque DOS Y DDOS, Apt, Código Malicioso, Manipulación De Datos, Saturación De Direcciones Mac O Ataques De Flooding De Mac., Ataque Ntp (Desincronización),
tecnología a implementar	Nessus, openvas, OWASP ZAP y nitko.

Fuente propia

Tabla 43 Plan pruebas hacking

Pruebas hacking	
Descripción	Realización de pruebas de hacking anuales sobre la plataforma del proyecto.
Activos afectados	Todos los equipos tecnológicos
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Arp Poison, Ataque De Diccionario O Fuerza Bruta, Ataque Web, : Exploit, Ataque Ntp (Desincronización), Password Craking, Ataque DOS Y DDOS, Apt, Código Malicioso, Manipulación De Datos, Saturación De Direcciones Mac O Ataques De Flooding De Mac., Ataque Ntp (Desincronización),
tecnología a implementar	contratación de pruebas de hacking ético con tercero sobre equipos seleccionados de la red

Fuente propia

Tabla 44 Plan Perímetro de seguridad físico definido

Perímetro de seguridad físico definido, Procedimientos de visitantes y mantenimientos de equipos de control de acceso	
Descripción	Definir los requisitos de seguridad física para los equipos PMU en el operador y en la sede de los agentes
Activos afectados	cableado, equipos físicos
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Conflictos personal proyecto, Ingeniería Social, Interceptación De Cableado, Daño Cableado Estructurado, Obsolescencia Técnica Y Tecnológica, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), Rotación O Cambio De Personal Gestor Del Proyecto, Suplantación De Identidad,
tecnología a implementar	procedimientos

Fuente propia

Tabla 45 Plan monitoreo de variables de salud

Monitoreo de variables como temperatura, estado de fuentes de energía, e debe aceptar debido a que estos fenómenos no son controlables	
Descripción	Implementación de monitorio vía SNMP
Activos afectados	Equipos Windows, PMU comerciales, sw, Firewall.
Riesgos / amenazas a mitigar	Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Obsolescencia Técnica Y Tecnológica, Obsolescencia Técnica Y Tecnológica, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc)
tecnología a implementar	Monitoreo por SOC por protocolo SNMP

Fuente propia

Tabla 46 Plan Asignación de recurso de seguridad segregación de funciones

Asignación de recurso seguridad al proyecto y segregación de funciones	
Descripción	Se debe asignar un recurso dedicado de seguridad al proyecto, esto con el fin de avanzar en las tareas de implementación de controles, análisis de seguridad, entrenamiento y capacitación del personal
Activos afectados	Personas
Riesgos / amenazas a mitigar	Conflictos personal proyecto, Rotación O Cambio De Personal Gestor Del Proyecto
Modelo de implementación	Personal contratado para tareas de seguridad

Fuente propia

Tabla 47 Plan Pólizas o seguros

Pólizas o seguros	
Descripción	Incluir la red de investigación en la póliza de ciber riesgo de la compañía
Activos afectados	todos los activos
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Acceso Lógico No Autorizado, Apt, Arp Poison, Arp Spoofing, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización), Ataque Sqlinyection, Ataque Web, Código Malicioso, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Conflictos personal proyecto, Envenenamiento De XML, Exploit, Ingeniería Social, Interceptación De Cableado, Daño Cableado Estructurado, Manipulación De Dato, Obsolescencia Técnica Y Tecnológica, Password Craking, Perdida O Fuga De Información, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), Ransomware, Rotación O Cambio De Personal Gestor Del Proyecto, Saturación De Direcciones Mac O Ataques De Flooding De Mac, Scanning, Suplantación De Identidad, Suplantación De Señales De Control
tecnología a implementar	Ajustes a póliza de ciber riesgo

Fuente propia

Tabla 48 Plan capacitación y entrenamiento en seguridad

Capacitación y entrenamiento en seguridad	
Descripción	Capacitación a todo el personal del proyecto en seguridad y ciberseguridad, así mismo entrenamiento según los roles desempeñados en el proyecto para mitigar riesgo ante ciber ataques
Activos afectados	Personas
Riesgos / amenazas a mitigar	Conflictos personal proyecto, Ingeniería Social, Rotación O Cambio De Personal Gestor Del Proyecto, Suplantación De Identidad
tecnología a implementar	Capacitación y entrenamiento

Fuente propia

Tabla 49 Plan Parches de seguridad

Parches de seguridad	
Descripción	Actualización de parches de seguridad sobre componentes que lo requieren, posterior definición de estrategia de parches.
Activos afectados	todos los activos
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Acceso Lógico No Autorizado, Apt, Arp Poison, Arp Spoofing, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización), Ataque Sqlinyection, Ataque Web, Código Malicioso, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Conflictos personal proyecto, Envenenamiento De XML, Exploit, Ingeniería Social, Interceptación De Cableado, Daño Cableado Estructurado, Manipulación De Dato, Obsolescencia Técnica Y Tecnológica, Password Craking, Perdida O Fuga De Información, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), Ransomware, Rotación O Cambio De Personal Gestor Del Proyecto, Saturación De Direcciones Mac O Ataques De Flooding De Mac, Scanning, Suplantación De Identidad, Suplantación De Señales De Control

tecnología a implementar	System center equipos Windows, manual equipos red y firewall.

Fuente propia

Tabla 50 Plan antimalware

Antimalware	
Descripción	Análisis de antimalware en equipos Windows o generación de listas blancas en caso de no ser posible su implementación.
Activos afectados	equipos Windows
Riesgos / amenazas a mitigar	Acceso Lógico No Autorizado, Apt, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización),Ataque Sqlinyection, Ataque Web, Código Malicioso, Envenenamiento De XML, Exploit, Manipulación De Datos, Obsolescencia Técnica Y Tecnológica, Password Craking, Ransomware, Scanning, Suplantación De Identidad, Suplantación De Señales De Control, XSS,
tecnología a implementar	Antimalware o listas blancas

Fuente propia

Tabla 51: Integrar red de supervisión a procedimiento internos del operador

Integrar red de supervisión a procedimiento internos del operador	
Descripción	Integrar la red de supervisión a los procedimientos de: Gestión de cambios Gestión de incidentes Gestión de la configuración Gestión de incidentes Gestión de recuperación y contingencia Procedimiento de notificación de alertas cibernéticas
Activos afectados	Todos los activos
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Acceso Lógico No Autorizado, Apt, Arp Poison, Arp Spoofing, Ataque De Diccionario O Fuerza Bruta, Ataque DOS Y DDOS, Ataque Ntp (Desincronización), Ataque Sqlinyection, Ataque Web, Código Malicioso, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Conflictos personal proyecto, Envenenamiento De XML, Exploit, Ingeniería Social, Interceptación De Cableado, Daño Cableado Estructurado, Manipulación De Dato, Obsolescencia Técnica Y Tecnológica, Password Craking, Perdida O Fuga De Información, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), Ransomware, Rotación O Cambio De Personal Gestor Del Proyecto, Saturación De Direcciones Mac O Ataques De Flooding De Mac, Scanning, Suplantación De Identidad, Suplantación De Señales De Control
tecnología a implementar	N/A

Fuente propia

Tabla 52 Integrar la red de supervisión a los controles y procedimientos de seguridad física del operador

Integrar la red de supervisión a los controles y procedimientos de seguridad física del operador	
Descripción	Este plan se basa en los numerales CIP-006-5: Cyber Security – Seguridad Física de los ciber activos BES y Acuerdo 788 Ciberseguridad del Sistema Eléctrico los cuales definen solicitan tener como mínimo:

	Perímetro de seguridad físico definido Implementar controles de acceso y definir procedimientos Procedimiento alerto relacionados con los elementos de control de acceso Esquema de almacenamiento para los registros de seguridad física Procedimientos de visitantes y mantenimientos de equipos de control de acceso
Activos afectados	Sedes operador, Cableado Operador
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Interceptación De Cableado, Daño Cableado Estructurado, Obsolescencia Técnica Y Tecnológica, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.)
tecnología a implementar	N/A

Fuente propia

Tabla 53: Sugerir a los agentes los controles de seguridad Física

Sugerir a los agentes los controles de seguridad Física	
Descripción	Este plan se basa en los numerales CIP-006-5: Cyber Security – Seguridad Física de los ciber activos BES y Acuerdo 788 Ciberseguridad del Sistema Eléctrico los cuales definen solicitan tener como mínimo: Perímetro de seguridad físico definido Implementar controles de acceso y definir procedimientos Procedimiento alerto relacionados con los elementos de control de acceso Esquema de almacenamiento para los registros de seguridad física Procedimientos de visitantes y mantenimientos de equipos de control de acceso
Activos afectados	Sedes agentes del SIN, Cableado agentes del SIN
Riesgos / amenazas a mitigar	Acceso Físico No Autorizado, Condiciones adversas o fenómenos de la naturaleza (Lluvia, terremoto, alud de tierra, granizada, alta temperatura, inundación, etc.), Interceptación De Cableado, Daño Cableado Estructurado, Obsolescencia Técnica Y Tecnológica, Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.)
tecnología a implementar	N/A

Fuente propia

4.2.3 Modelo de ciberseguridad

El modelo de ciberseguridad definido para la red de PMU se presenta en la tabla 54 el cual debe aplicarse para la protección de la red de supervisión futura, este aplica a cada uno de sus elementos actuales como las PMU y elementos futuros que se agreguen a la red.

Tabla 54: modelo de ciberseguridad

Modelo de ciberseguridad basado en Nist Cibersecurity Framework, ISO 27001:2013 y NERCCIP		
	Gestión de activos	Identificar y mantener actualizado con periodicidad anual el inventario de activos (equipos, software hardware, mapas de comunicación, flujos de datos de datos e interacciones entre activos) de la red y se deben clasificar según su criticad (activos físicos, ciber activos y ciber activos críticos) para todos los elementos del sistema de supervisión por PMU.
		Se identifican los roles y responsabilidades de seguridad para la todo el personal que labora en esta, incluyendo los terceros, se debe nombrar

IDENTIFICAR: La organización identifica todos los elementos necesarios para su protección ante ataques cibernéticos		oficialmente un responsable de ciberseguridad para la red de supervisión por PMU.
	Infraestructuras críticas y grupos de interés	Se identifica y comunica el lugar de la organización en la infraestructura crítica y su sector industrial, se participa en el inventario de infraestructuras críticas de Colombia del Comando conjunto cibernético.
		Se establece contacto con las autoridades y grupos de interés de infraestructura critica que apoyan la gestión de incidentes y la notificación de nuevas amenazas, se debe reportar los incidentes de la red a estos grupos especializados.
	Políticas y cumplimiento	La política de seguridad de la compañía debe cubrir los elementos de la red de supervisión.
		Identificar y mantener los requisitos legales y regulatorios de la red de supervisión.
	Gestión de riesgos	Se diseña, implementa y mantienen un proceso continuo de gestión de riesgos, donde se identifican causas, impacto y tratamiento para todos los elementos del inventario de activo incluyendo personal.
		Se identifican los riesgos sobre la cadena de suministro, se les hace monitoreo, verificación y pruebas de seguridad de cumplimiento de controles.
		Se identifican y gestionan las vulnerabilidades de todos los elementos de la plataforma de manera periódica, se deben incluir las alertas y notificaciones de inteligencia de grupos especializados.
PROTEGER: La organización diseña procedimientos e implementa controles para mitigar los riesgos identificados con el fin de proteger la organización	Gestión de identidades y control de acceso	Se identifican y gestionan todas las identidades y accesos lógicos, así como las conexiones que se requiere para la operación de la red de supervisión, estas se deben validar de manera periódica y se debe tener constancia de estas.
		Se implementa segmentación de red para los equipos críticos basado en los criterios de NERCCIP, donde se tenga la mínima interacción y privilegios con los equipos PMU.
		Se identifican y gestionan todas las identidades de accesos físicos, estas se deben validar de manera periódica y se debe tener constancia de estas.
		Identificar, monitorear y gestionar todas las conexiones remotas necesarias para la operación.
	Sensibilización y entrenamiento	Diseñar, establecer e implementar programas de concientización periódicos a todos los niveles, y diferenciados por roles, incluyendo terceros, esta capacitación se deben basar en los criterios de NERCCIP
		Desarrollar planes de capacitación técnica al personal de la red de supervisión, incluyendo terceros, haciendo énfasis en los conceptos de seguridad en tecnologías de operación y respuesta a incidentes
	Seguridad de los datos	Diseñar, implementar y mantener mecanismos para proteger los datos en reposo y tránsito, garantizando la integridad de la información, adicionalmente se deben implementar controles para evitar la fuga de información y la eliminación segura de datos
		Diseñar, implementar y mantener separación de los ambientes productivos y no productivos
	Procedimientos	Establecer procedimiento y líneas base de seguridad de cada uno de los elementos de la red, se debe hacer verificación periódica del cumplimiento de estas.
		Establecer e implementar procedimiento de Gestión de cambios sobre los activos de la red que permitan validar la seguridad de estos tras tener cabios de configuración o cambios de tecnología
		Establecer e implementar procedimiento de copia de seguridad
		Establecer e implementar procedimiento de respuesta a incidentes, recuperación, continuidad de los elementos de la red de supervisión.
		Establecer y configurar requisitos de seguridad en desarrollo, adquisidor e implementación para productos, así como pruebas de seguridad para aplicativos existentes

		Establecer e implementar procedimientos de Mantenimiento local y remoto controlado y supervisado de los elementos de la red de supervisión
		Se establecen procedimientos y controles de seguridad física sobre los distintos elementos de red
	Tecnología de protección	Se identifican todos los log y registro de auditoria necesarios para la gestión de incidentes
		Se restringen y monitorea la utilización de medios removibles
		Se implementan, monitorean y se gestionan elementos de seguridad para minimizar el riesgo de ataques cibernéticos, así como se identifican y configuran protocolos y servicios.
		Se implementan controles de seguridad física para la protección de la red supervisión.
DETECTAR: La organización define la estrategia de detección de incidentes de ciberseguridad	Monitoreo continuo	Se monitorean en tiempo real los distintos dispositivos de la red de supervisión acorde al procedimiento de gestión de incidentes.
		Se realiza análisis de eventos de seguridad, se correlacionan los datos determinando su impacto, nivel de respuesta y umbrales de alertas.
		Se supervisa la actividad del proveedor de servicios externos para detectar posibles eventos de ciberseguridad.
		Se realizan análisis de vulnerabilidades periódicas y pruebas especializadas de seguridad sobre los elementos de la red de supervisión.
		Se valida el procedimiento de gestión de incidentes y se realiza mejora continua sobre este.
RESPONDER: La organización define la estrategia para responder ante incidentes de seguridad	Respuesta, Mitigación y mejora continua	Se debe conformar equipo de respuesta a incidentes para responder ante posibles ataques.
		Los eventos de seguridad se notifican acorde al plan de respuesta de incidentes, se realizan los escalamientos necesarios y se intercambia información con entes externo.
		Actualizar las estrategias de plan de respuesta ante incidentes continuamente.
RECUPERAR: La organización define la estrategia de recuperación ante incidentes cibernéticos	Plan de recuperación y mejoramiento	Activar el plan de recuperación durante y después de un incidente sobre la red de supervisión.
		Actualizar los planes de recuperación con las lecciones aprendidas.
		Las actividades de recuperación se comunican a las partes interesadas internas y a los equipos ejecutivos y de gestión.
		Gestionar la reputación y las relaciones publicas después de un evento cibernético sobre infraestructuras críticas.

Fuente propia

4.3 Valorar la implementación del modelo

4.3.1 Verificación y documentación de las condiciones actuales del ambiente de investigación

Modelo de red después de implementación de controles:

En consideración de la implementación de algunos de los controles (para reducir los niveles de riesgos) en el ambiente de ISAAC, se presentaron cambios significativos en el esquema de red el cual se muestra en la figura 10, esto cambio fueron:

- Definición de nuevos segmentos de red y direccionamiento
- Asignación de nuevo router que permite el enrutamiento de las redes nacional de producción y nacional de pruebas con las redes corporativas y servidores de pruebas.
- Ajuste en la política de firewall mejorando los niveles de segmentación
- Una red nacional producción donde se encuentran solo las PMU comerciales.
- Una red Nacional de Pruebas donde se encuentran aisladas las PMU tipo Prototipo
- Una red de servidores de pruebas donde se encuentra el servidor de seguridad y servidor controlador de domino.

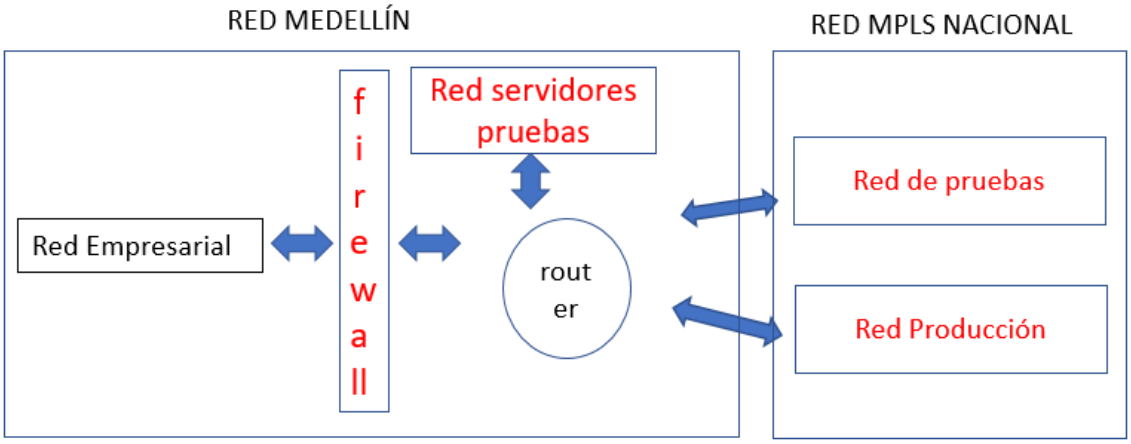


Figura 10 Nuevo esquema de red. Fuente propia

Adicionalmente se realizó un escaneo de equipos para validar el inventario y evidenciar los equipos existentes en el ambiente, como resultado de este escaneo se presenta la tabla 55 con los activos actuales.

Tabla 55 Inventario de equipos red ISAAC

#	Tipo	Departamento	Marca	SO	RED
1	PMU	Norte de Santander	Comercial 1	Propietario	Red nacional Producción
2	PMU	Cundinamarca	Comercial 2	Propietario	Red nacional Producción
3	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
4	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
5	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
6	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
7	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
8	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
9	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
10	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
11	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
12	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
13	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
14	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
15	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
16	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
17	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
18	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
19	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
20	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
21	PMU	Atlántico	Comercial 3	Propietario	Red nacional Producción
22	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
23	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
24	PMU	Cundinamarca	Comercial 2	Propietario	Red nacional Producción
25	PMU	Córdoba	Comercial 2	Propietario	Red nacional Producción
26	PMU	Boyacá	Comercial 4	Propietario	Red nacional Producción
27	PMU	Risaralda	Comercial 4	Propietario	Red nacional Producción
28	PMU	Norte de Santander	Comercial 4	Propietario	Red nacional Producción
29	PMU	Santander	Comercial 4	Propietario	Red nacional Producción
30	PMU	Valle del auca	Comercial 4	Propietario	Red nacional Producción
31	PMU	Tolima	Comercial 4	Propietario	Red nacional Producción
32	PMU	Córdoba	Comercial 4	Propietario	Red nacional Producción
33	PMU	Córdoba	Comercial 4	Propietario	Red nacional Producción
34	PMU	Meta	Comercial 4	Propietario	Red nacional Producción
35	PMU	Santa Rosa, Bolívar	Comercial 4	Propietario	Red nacional Producción
36	PMU	Cundinamarca	Comercial 4	Propietario	Red nacional Producción
37	PMU	cesar	Comercial 4	Propietario	Red nacional Producción
38	PMU	Antioquia	Comercial 4	Propietario	Red nacional Producción
39	PMU	Nariño	Comercial 4	Propietario	Red nacional Producción
40	PMU	Antioquia	Comercial 4	Propietario	Red nacional Producción
41	PMU	Boyacá	Comercial 2	Propietario	Red nacional Producción
42	PMU	Cundinamarca	Comercial 2	Propietario	Red nacional Producción
43	PMU	Nariño	Comercial 2	Propietario	Red nacional Producción
44	PMU	Antioquia	Comercial 2	Propietario	Red nacional Producción
45	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
46	PMU	Boyacá	Comercial 4	Propietario	Red nacional Producción
47	PMU	Boyacá	Comercial 4	Propietario	Red nacional Producción
48	PMU	Vichada	Comercial 4	Propietario	Red nacional Producción
49	PMU	Norte de Santander	Comercial 4	Propietario	Red nacional Producción
50	PMU	Antioquia	Comercial 4	Propietario	Red nacional Producción
51	servidor 11	Atlántico	N/A	Windows	Red nacional Producción
52	servidor 12	Atlántico	N/A	Windows	Red nacional Producción

53	servidor 13	Atlántico	N/A	Windows	Red nacional Producción
54	PMU	Cesar	Comercial 5	Propietario	Red nacional Producción
55	PMU	Atlántico	Comercial 2	Propietario	Red nacional Producción
56	PMU	Cesar	Comercial 5	Propietario	Red nacional Producción
57	PMU	Pasto	Comercial 2	Propietario	Red nacional Producción
58	PMU	Caldas	Comercial 2	Propietario	Red nacional Producción
59	router	sin identificar	N/A	Propietario	Red nacional Producción
60	router	sin identificar	N/A	Propietario	Red nacional Producción
61	router	sin identificar	N/A	Propietario	Red nacional Producción
62	router	sin identificar	N/A	Propietario	Red nacional Producción
63	servidor	Norte Santander	N/A	Windows	Red nacional Producción
64	Router	Antioquia	N/A	Propietario	Red nacional Producción/red pruebas
65	firewall	sin identificar	N/A	Propietario	Red nacional Producción/red pruebas
66	PMU	Huila	Prototipo	Windows 10	red nacional pruebas
67	PMU	Cundinamarca	Prototipo	Windows 10	red nacional pruebas
68	PMU	Cundinamarca	Prototipo	Windows 10	red nacional pruebas
69	PMU	Córdoba	Prototipo	Windows 7	red nacional pruebas
70	PMU	Antioquia	Prototipo	Windows 10	red nacional pruebas
71	PMU	Risaralda	Prototipo	Windows 10	red nacional pruebas
72	PMU	Valle del Cauca	Prototipo	Windows 10	red nacional pruebas
73	PMU	Bolívar	Prototipo	Windows 10	red nacional pruebas
74	PMU	Córdoba	Prototipo	Windows 7	red nacional pruebas
75	PMU	Manizales	Prototipo	Windows 10	red nacional pruebas
76	PMU	Atlántico	Prototipo	Windows 10	red nacional pruebas
77	PMU	Córdoba	Prototipo	Windows 7	red nacional pruebas
78	PMU	valle del cauca	Prototipo	Windows 10	red nacional pruebas
79	PMU	Antioquia	Comercial4	Propietario	Red nacional Producción
80	servidor 1	Antioquia	N/A	Windows	red nacional pruebas
81	servidor 2	Antioquia	N/A	Windows	red nacional pruebas
82	servidor 3	Antioquia	N/A	Windows	red nacional pruebas
83	servidor 4	Antioquia	N/A	Windows	red nacional pruebas
84	servidor 5	Antioquia	N/A	Linux	red nacional pruebas
85	servidor 6	Antioquia	N/A	Windows	red nacional pruebas
86	servidor 7	Antioquia	N/A	Windows	red nacional pruebas
87	servidor 8	Antioquia	N/A	Windows	red nacional pruebas
88	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
89	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
90	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
91	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
92	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
93	eq comunicación	sin identificar	N/A	Propietario	red nacional pruebas
94	equipo industrial	sin identificar	N/A	Propietario	red nacional pruebas
95	equipo industrial	sin identificar	N/A	Propietario	red nacional pruebas
96	equipo industrial	sin identificar	N/A	Propietario	red nacional pruebas
97	servidor	Antioquia	N/A	Linux	red nacional pruebas
98	servidor	Antioquia	N/A	Linux	red nacional pruebas
99	servidor	Antioquia	N/A	Linux	red nacional pruebas
100	Alienvaultt	Antioquia	N/A	Linux	red nacional pruebas
101	Servidor dominio	Antioquia	N/A	Windows	red nacional pruebas

Fuente propia

Se destacan dos equipos nuevos: servidor de domino y router de comunicaciones, fundamentales para los esquemas de protección definidos.

El número de PMU tipo prototipo son 13, se logró realizar cambio de 10 PMU con sistema operativo Windows y continúan 3 PMU con sistema operativo pendiente por actualizar.

4.3.2 Implementar los controles definidos acorde al mapa de riesgos sobre las PMU

Se representa a continuación el resumen de estado de avance de implementación de controles en la tabla 56

Tabla 56 Resumen de implementación de planes

Nombre plan	Porcentaje implementado	Que se ha implementado	Que falta implementar	Fecha probable implementación
Segmentación de red	100%	Cambio re router y enrutamiento Nuevo esquema de segmentación Ajustes en firewall	N/A	N/A
Cambio de sistema operativo obsoleto	77%	Cambio de sistema operativo Windows 7 y XM por Windows 10	Faltan cambiar 3 PMU que tienen Windows 7, se decide asumir el riesgo de estas y poner controles complementarios	N/A, debido a que la red de pruebas se dará de baja a finales de 2020
Línea base seguridad PMU comerciales	100%	Se realiza: cambios de contraseña por defectos ajuste en puertos y servicios no inseguros y no utilizados segregación de roles reporte de log	N/A	N/A
Controlador de domino monitoreo por el SOC	100%	Implementación controlador dominio red de pruebas, generación de GPO de usuarios y equipos	N/A	N/A
Monitorio SOC	100%	Se implementa monitoreo de las distintas redes: monitoreo firewall, de syslog equipo red y servidores Linux, instalación agente OSSEC equipos Windows, análisis de portmirror	N/A	N/A
servicio de ciber inteligencia del SOC	100%	Se incluye en tráfico en la plataforma de cibreinteligencia	N/A	N/A

Actualizaciones de firmware	100%	Se actualiza firmware de PMU y equipos de red	N/A	N/A
pruebas hacking	50	Se realizan pruebas a servidores críticos y a PMU prototipo	Pendiente PMU Comerciales	Julio 2020
Perímetro de seguridad físico definido	100%	Se ajustan los perímetros en el operador y se hacen recomendaciones a los agentes	N/A	N/A
Estado salud equipos	100%	Se implementa monitoreo vía SMNP de toda la plataforma y se configuran parámetros de alertas	N/A	N/A
Asignación de recurso seguridad al proyecto y segregación de funciones	100%	Se asigna persona de la compañía dedicada 50% del tiempo al proyecto	N/A	N/A
capacitación y entrenamiento en seguridad	100%	Se realizan capacitaciones al personal y se entrena en seguridad	N/A	N/A
Pólizas o seguros	100%	Se incluye la red de investigación en la póliza de ciber riesgo de la compañía	N/A	N/A
Gestión de parches	80%	Se actualizan los equipos y se define estrategia de parches en un	Faltaron las 3 PMU con Windows 7, se asume el riesgo	N/A
antimalware	100%	Se define línea base para antimalware basado en excepciones.	N/A	N/A
Integrar red de supervisión a procedimientos internos del operador	100%	Se integra la red de supervisión a los procedimientos de: Gestión de cambios Gestión de incidentes Gestión de la configuración Gestión de incidentes Gestión de recuperación y contingencia Procedimiento de notificación de alertas cibernéticas	N/A	N/A
Integrar la red de supervisión a los controles y procedimientos de	100%	Integración de la red a los controles de seguridad Física	N/A	N/A

seguridad física del operador				
Sugerir a los agentes los controles de seguridad Física	100%	Notificación al os agentes de los controles sugeridos para dar cumplimiento a los controles de NERCCIP	N/A	N/A

Nota: N/A quiere decir no aplica, porque el control ya fue implementado

Fuente propia

4.3.3 Verificar nuevamente los niveles de riesgos

Una vez implementado los controles se procede nuevamente a hacer evolución de riesgo de la red la cual da como resultado una disminución de los niveles de riesgo de la red ISAAC.

Los riesgos que continua en nivel ***inaceptable tabla 57***, se plantea una estrategia a mediano y largo plazo, así mismo debe ser transferido a otras áreas para que apoyen su desarrollo, tal es el caso de:

- Posibilidad que la amenaza: Ingeniería Social, afecte el activo: Personas
- Posibilidad que la amenaza: Rotación O Cambio De Personal Gestor Del Proyecto, afecte el activo: Personas.

Dichos riesgos deben ser apoyados por las áreas de recursos humanos y comunicaciones interna, para lo cual, se debe desarrollar un plan de cultura y sensibilización que logre reducir los riesgos de exposición.

Tabla 57 Riesgos inaceptables después de implementación de controles

RIESGOS ALTOS Considerando los controles actuales	TRATAMIENTO			
	Aceptarlo	Evitarlo	Controlarlo	Transferirlo
(64) -Posibilidad que la amenaza: Ingeniería Social, afecte el activo: Personas	x			x
(66) -Posibilidad que la amenaza: Interceptación De Cableado, afecte el activo: Cableado agentes del SIN				x
(68) -Posibilidad que la amenaza: Daño Cableado Estructurado, afecte el activo: Cableado agentes del SIN				x
(91) -Posibilidad que la amenaza: Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), afecte el activo: Sedes agentes del SIN				x
(92) -Posibilidad que la amenaza: Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), afecte el activo: Cableado Operador				x
(93) -Posibilidad que la amenaza: Problemas De Seguridad Publica (asonada, vandalismo, terrorismo, mitin, etc.), afecte el activo: Cableado agentes del SIN				x
(96) -Posibilidad que la amenaza: Rotación O Cambio De Personal Gestor Del Proyecto, afecte el activo: Personas	x			x

Fuente propia

El nuevo mapa de calor después de controles se presenta en la figura 11 en la cual se puede observar que ya no se encuentran riesgos en color rojo denominados inadmisibles

	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3		X			
Improbable	2	X	X	XXX	X	X
Raro	1	XX	XX	XX	XX	XXX

Figura 11 Mapa de calor después de implementación de controles. Fuente propia

La distribución del nuevo mapa queda reflejada en la figura 12

DISTRIBUCIÒN PORCENTUAL

ZONA	%	Total riesgos
Aceptable	21.49	26
Tolerable	72.73	88
Inaceptable	5.79	7
Inadmisible	0.00	0

Figura 12 Distribución de los riesgos. Fuente propia

4.3.4 Análisis de comparativo de Riesgo

La figura 13 muestra el cuadro comparativo antes y después de la implementación de controles, lo cual presenta un escenario totalmente distinto a la inicial, los riesgos de tipo inadmisibles se mitigaron en su totalidad, los riesgos inaceptables actuales son 7 los cuales representa un 5,79%, estos riesgos se aceptaron por la alta gerencia o se trasfirieron a pólizas y seguros, los riesgos inaceptables se pueden observar en la tabla 55.

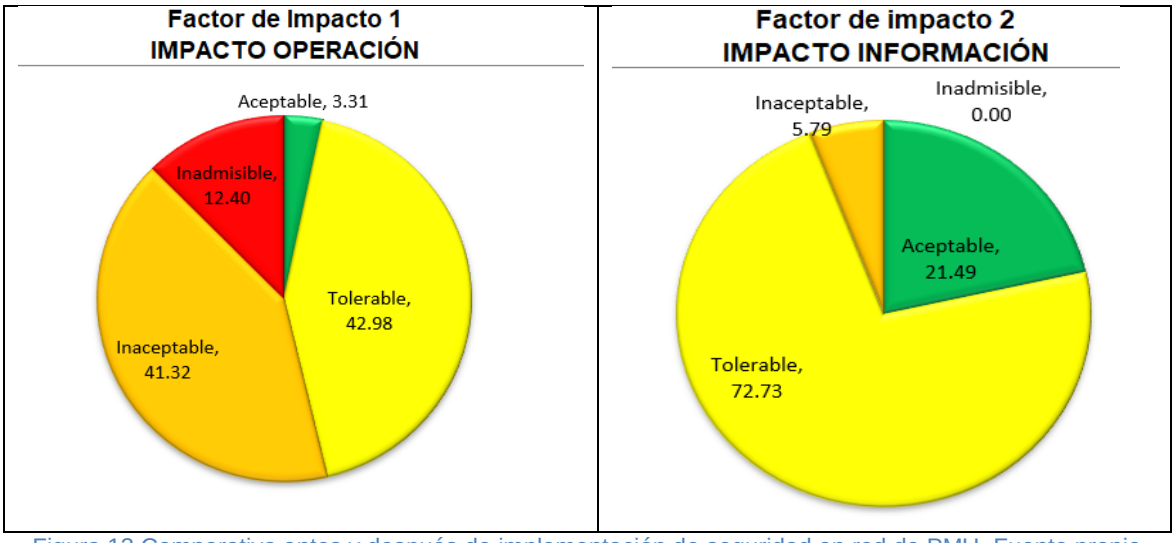


Figura 13 Comparativo antes y después de implementación de seguridad en red de PMU. Fuente propia

Se presenta disminución de los riesgos inadmisibles de un 12,40% a 0% y disminución de los riesgos inaceptables de un 41.35% a 5,79% lo que demuestra que lo panes de tratamiento cumplieron su objetivo.

Se presenta un aumento en el nivel de riesgo tolerable de 42,98% a 72,73% y de los riesgos aceptables de 3,31% a 21,49% estos riesgos deben estar en constante monitoreo y vigilancia mediante los planes que fueron definidos periódicos.

5. Conclusiones y recomendaciones

5.1 Conclusiones

Contemplar un modelo de ciberseguridad basado en las 5 etapas (identificar, proteger, detectar, responder y recuperar) para el proyecto ISAAC, es fundamental para la reducción de los niveles de exposición al riesgo. El modelo debe contemplar en su fase de implementación todo un proceso de capacitación a los diferentes empleados y partes interesadas, que permita el conocimiento de dichas fases y cómo actuar cuando se presente una eventualidad. Sumado a esto, mantener en constante monitoreo los equipos y sistemas, así como un procedimiento de validación de requisitos de seguridad cuando equipos y sistemas nuevos deban ser incluidos en el proceso o se deban conectar a una red de computadores.

Con respecto al cumplimiento de los objetivos, par el objetivo 1 “Establecer los posibles ataques y vulnerabilidades sobre dispositivos de supervisión PMU, con el fin de estimar los riesgos asociados a ciberataques sobre dispositivos de supervisión PMU.” Se logró de manera exitosa como se muestra en el numeral 4.1.4 Evaluación de riesgos el nivel de riesgos para la red ISAAC donde Se encuentra que un 16,55% de los riesgos son inadmisibles, lo que indica que el proyecto está en alto riesgo y es susceptible a presentarse un ataque informático, los elementos que más preocupan son la falta de controles sobre las PMU prototipo con sistema operativo Windows xp y Windows 7 las cuales ya tienen sistema operativo obsoleto, adicionalmente se nota una falta de hardening sobre la PMU comerciales lo cual las hace susceptibles. Este tipo de riesgo debe mitigarse los antes posible, los riesgos inaceptables representan un 41,73 % del total de los riesgos los cuales se deben mitigar en un corto plazo. En términos generales el ambiente de investigación de la red ISAAC sobre la cual se realizó el análisis de riesgo es altamente vulnerable y tienen un nivel de impacto alto que puede terminar con el proyecto.

En el objetivo 2 “Definir el plan de tratamiento de riesgos basados en los riesgos encontrados, que reduzcan los niveles de impacto sobre los dispositivos de supervisión PMU”. Se logró de manera exitosa mediante el numeral 4.2.1 Homologación de normas y planes de tratamiento (ISO 27001, NIST CSF y NERC CIP) la cual permitió realizar el cruce de esta normas e identificar los puntos clave

de estas, numeral 4.2.2, Definición de planes de tratamiento por medio de la cual se definió los planes que se deben implementar para disminuir el nivel de riesgo del proyecto y el numera 4.2.3 Definición del modelo de ciberseguridad, el cual establece el modelo o guía seguir en la seguridad de la red de ISAAC por parte del operador y de los agentes del SIN que interactúan con la red.

En el objetivo 3 "Valorar la implementación del plan de tratamiento de riesgos a través de la implementación de un ambiente de prueba controlado, que permita obtener los resultados del modelo propuesto y el impacto de los controles de seguridad sobre las funcionalidades de los equipos" se logra de manera exitosa por medio del numeral 4.3.1 Verificación y documentación de las condiciones actuales del ambiente de investigación presenta un nuevo modelo de red y la incursión de nuevos equipos que brindan seguridad a la red, el numeral 4.3.2 Implementar los controles definidos acorde al mapa de riesgos sobre las PMU que presenta el estado de implementaciones con sus alcances y compromisos y el numeral 4.3.3 Verificar nuevamente los niveles de riesgos en la cual se presenta que ya no existen riesgos inadmisibles producto de la implementación de controles y los riesgo inaceptables se reduce considerablemente y solo se presenta 7, los cuales están asociados en su gran mayoría a : Problemas de seguridad pública, ingeniería social y riesgo asociados a seguridad física, esos riesgos ya fueron aceptados y cubiertos en la póliza de ciber riesgo de la compañía, adicionalmente se puede observar el Enel numeral 4.3.4 Análisis de comparativo de Riesgo ele estado inicial del proyecto vs el estado final después de la definición del modelo y la implementación de planes de tratamiento.

Con respecto al objetivo general del proyecto "*Diseñar un modelo de ciberseguridad de las Unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) para sistema eléctrico Nacional, con el fin de reducir los niveles de exposición a ataques informáticos*" se logró de manera exitosa por medio del cumplimiento de los objetivos específicos.

5.2 Recomendaciones

- Conservar el modelo de segmentación de red que independiza los elementos de investigación de los de producción, el no conservar el modelo de segmentación compromete el ambiente de producción.
- Conservar y potenciar el modelo de monitoreo de la seguridad por medio del centro de operación de seguridad - SOC de XM, haciendo énfasis en los protocolos industriales.
- Potenciar los modelos de cooperación y ciber inteligencia sobre la red ISAAC con el fin de tener alertar tempranas a nivel mundial sobre redes de este tipo.
- Continuar los planes de remediación periódicos como lo son el análisis de vulnerabilidades y la prueba de hacking ético sobre la red, el no hacerlos bajaría el nivel de seguridad.
- Definir un mecanismo futuro para exigir que los agentes del sistema eléctrico y el operador cumplen con el modelo se seguridad definido.
- Se deben hacer trabajos similares a esta cada vez que se incorporen nueva tecnología en la red de supervisión.

Bibliografía

[1] Consejo de la Unión Europea, "Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008 , sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (Texto pertinente a efectos del EEE)," *Publicaciones UE*, 2008. [Online]. Available: https://publications.europa.eu/es/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/.

[2] XM, "Que hacemos," *Que hacemos*, 2019. [Online]. Available: http://www.xm.com.co/corporativo/Paginas/Nuestra-empresa/que-hacemos.aspx.

[3] XM, "Proyecto Isaac. Autor corporativo," *Proyecto Isaac. Autor corporativo*, 2018. [Online]. Available: http://informesanuales.xm.com.co/2013/SitePages/sostenibilidad/4-2-2-8-Iniciativa-Colombia-Inteligente.aspx. [Accessed: 10-Sep-2019].

[4] ACIS, "Ciber riesgos, un riesgos sitémico. Revista sistemas.," *Ciber riesgos, un riesgos sitémico. Revista sistemas.*, 2019. [Online]. Available: https://acis.org.co/archivos/Revista/Sistemasedicion151.pdf.

[5] R. A. Leon and J. E. Gomez, "Colombian National Defense System against large scale events," *IEEE Power Energy Soc. Gen. Meet.*, pp. 1–6, 2011.

[6] D. L. and S. S. R. Khan, K. McLaughlin, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," *2016 IEEE Power Energy Soc. Gen. Meet.*, vol. pp. 1-5., 2016.

[7] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[8] DNP Departamento de Planeacion Nacional, "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL," *POLÍTICA NACIONAL DE SEGURIDAD DIGITAL*, 2016. [Online]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.

[9] Centro Ciberseguridad inustrial, "LA CIBERDEFENSA EN COLOMBIA," *LA CIBERDEFENSA EN COLOMBIA*, 2017. [Online]. Available: https://www.cci-es.org/documents/10694/468834/3.+CCOC+PLAN+NACIONAL.pdf/84da120e-3bd6-478c-99c8-1f88c3543355;jsessionid=5E61914D5E08633E7DD315CB4A68FC94?version=1.0.

[10] Consejo Nacional de Operación, "Quienes somos," *Quienes somos*. [Online]. Available: https://www.cno.org.co/content/quienes-somos.

[11] Corporation North American Electric Reliability, "CIP Standards," *CIP Standards*, 2017. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[12] Consejo Nacional de Operación, "Acuerdo 1241 Por el cual se aprueba la actualización de la Guía de Ciberseguridad," *Acuerdo 1241 Por el cual se aprueba la actualización de la Guía de Ciberseguridad*, 2019. [Online]. Available: https://www.cno.org.co/content/acuerdo-1241-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad.

[13] NIST, "CYBERSECURITY FRAMEWORK," *CYBERSECURITY FRAMEWORK*, 2018. [Online]. Available: https://www.nist.gov/cyberframework/framework.

[14] Icontec internacional, *Norma técnica Colombiana NTC ISO/IE 27005:2011, TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN*. 2011.

[15] L. Spitzner, "Applying Security Awareness to the Cyber Kill Chain," *SANS Security Awareness*, 2019. [Online]. Available: https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain.

[16] ISO-IEC, *Norma técnica NTC-ISO-IEC 27001:2013. Gestión de la seguridad de la información. Manual de referencia. ISBN impreso: 978-958-8585-53-6*. 2015.

[17] F. M. Sousa and P. M. Silva, "22 nd International Conference on Electricity Distribution Paper 0927 22 nd International Conference on Electricity Distribution," no. 0201, pp. 10–13, 2013.

[18] R. Cespedes, R. A. Leon, H. Salazar, M. E. Ruiz, R. Hidalgo, and D. Mejia, "An appraisal of the challenges and opportunities for the Colombia Inteligente Program implementation," *IEEE Power Energy Soc. Gen. Meet.*, pp. 1–6, 2012.

[19] C. W. Axelrod, "Managing the risks of cyber-physical systems," *2013 IEEE Long Isl. Syst. Appl. Technol. Conf.*, pp. 1–6, 2013.

[20] K. Gajrani and A. Bhargava, "Cyber Security Solution for Wide Area Measurement Systems in Wind Connected Electric Grid," pp. 1–5, 2013.

[21] S. Pal, B. Sikdar, and J. H. Chow, "An Online Mechanism for Detection of Gray-Hole Attacks on PMU Data," *IEEE Trans. Smart Grid*, 2018.

[22] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and Implementation of Security Gateway for Synchrophasor Based Real-Time Control and Monitoring in Smart Grid," vol. 5, no. ii, 2017.

[23] Z. Mao, T. Xu, and T. J. Overbye, "Real-time detection of malicious PMU data," in *2017 19th International Conference on Intelligent System Application to Power Systems, ISAP 2017*, 2017.

[24] D. R. Gurusinghe, D. Ouellette, and A. D. Rajapakse, "Development of a test platform for synchrophasor applications with real-time digital simulator," in *1st International Conference - EECon 2016: 2016 Electrical Engineering Conference*, 2017.

[25] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *IEEE Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2016 - This Workshop is Part of the CPS Week 2016*, 2016.

[26] H. M. Khalid and J. C. H. Peng, "A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks," *IEEE Trans. Smart Grid*, 2016.

[27] J. Zhao, G. Zhang, and R. A. Jabr, "Robust Detection of Cyber Attacks on State Estimators

Using Phasor Measurements," *IEEE Trans. Power Syst.*, vol. 32, no. 3, pp. 2468–2470, 2017.

[28] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs," 2015.

[29] C. Beasley, G. K. Venayagamoorthy, and R. Brooks, "Cyber security evaluation of synchrophasors in a power system," in *2014 Clemson University Power Systems Conference, PSC 2014*, 2014.

[30] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mob. Comput.*, vol. 13, no. 8, pp. 1746–1759, 2014.

[31] A. Mazloomzadeh, O. A. Mohammed, and S. Zonouzsaman, "Empirical development of a trusted sensing base for power system infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2454–2463, 2015.

[32] M. Nakao, S. Loo, L. Melville, and S. E. Laboratories, "Integrating Modern Substation Automation Systems With Enterprise-Level Management," pp. 557–562, 2015.

[33] C. Sun, J. Hong, and C. Liu, "A Co-Simulation Environment for Integrated Cyber and Power Systems," pp. 133–138, 2015.

[34] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, 2015.

[35] K. Zhu, "New Trends in the Development of Wide-Area Damping Control Systems," pp. 1–6, 2014.

[36] I. Darwish, O. Igbe, O. Celebi, T. Saadawi, and J. Soryal, "Smart Grid DNP3 Vulnerability Analysis and Experimentation," *2015 IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, pp. 141–147, 2015.

[37] I. Darwish, O. Igbe, and T. Saadawi, "Experimental and theoretical modeling of DNP3 attacks in smart grids," *Sarnoff Symp. 2015 36th IEEE*, pp. 155–160, 2015.

[38] X. Zhong, I. Jayawardene, G. K. Venayagamoorthy, and R. Brooks, "Denial of Service Attack on Tie-Line Bias Control in a Power System With PV Plant," *IEEE Trans. Emerg. Top. Comput. Intell.*, 2017.

[39] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications," *IEEE Systems Journal*, 2017.

[40] P. Gao *et al.*, "Identification of successive 'Unobservable' cyber data attacks in power systems through matrix decomposition," *IEEE Trans. Signal Process.*, vol. 64, no. 21, pp. 5557–5570, 2016.

[41] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," *2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, pp. 1–5, 2015.

[42] J. Jayachandrabensam and J. D. Anunciya, "Implementation Against DoS Attacks," 2015.

[43] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," *2015 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, pp. 1–5, 2015.

[44] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan, "Distributed Framework for Detecting PMU Data Manipulation Attacks With Deep Autoencoders," *IEEE Transactions on Smart Grid*, 2018.

[45] J. Zhao, L. Mili, and M. Wang, "A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures," *IEEE Trans. Power Syst.*, vol. 8950, no. c, pp. 1–10, 2018.

[46] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU Placement in Electric Transmission Networks for Reliable State Estimation Against False Data Injection Attacks," *IEEE Internet Things J.*, 2017.

[47] S. Pal, B. Sikdar, and J. Chow, "Detecting data integrity attacks on SCADA systems using limited PMUs," in *2016 IEEE International Conference on Smart Grid Communications, SmartGridComm 2016*, 2016, pp. 545–550.

[48] P. Arunagirinathan, R. Brooks, G. Venayagamoorthy, L. Yu, and Y. Fu, "Side Channel Analysis of Multiple PMU Data in Electric Power Systems," 2015.

[49] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," *2014 North Am. Power Symp. NAPS 2014*, pp. 1–6, 2014.

[50] M. Dehghani, "Integrity Attack Detection in PMU Networks Using Static State Estimation Algorithm," *PowerTech*, 2015.

[51] D. Deka, R. Baldick, and S. Vishwanath, "Optimal Data Attacks on Power Grids : Leveraging Detection & Measurement Jamming," 2015.

[52] M. Garcia, A. Giani, and R. Baldick, "Smart Grid Data Integrity Attacks: Observable Islands," *IEEE Power Energy Soc. Gen. Meet. 2015*, 2015.

[53] Z. Hu and Y. Wang, "False Data Injection Attacks Identification for Smart Grids," pp. 139–143, 2015.

[54] P. Kundu and A. K. Pradhan, "Enhanced Protection Security using System Integrity Protection Scheme (SIPS)," *IEEE Trans. Power Deliv.*, vol. PP, no. 99, pp. 1–1, 2015.

[55] S. Pal, B. Sikdar, and J. Chow, "Real-time detection of packet drop attacks on synchrophasor data," *2014 IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2014*, pp. 896–901, 2015.

[56] S. Pal and B. Sikdar, “A Mechanism for Detecting Data Manipulation Attacks on PMU Data,” pp. 253–257, 2014.

[57] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, “GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment,” *IET Cyber-Physical Syst. Theory Appl.*, vol. 2, no. 4, pp. 180–187, 2017.

[58] M. N. Aman, K. Javed, B. Sikdar, and K. C. Chua, “Detecting data tampering attacks in synchrophasor networks using time hopping,” in *IEEE PES Innovative Smart Grid Technologies Conference Europe*, 2017.

[59] K. Y. Chen *et al.*, “Risk Analysis of GPS-Dependent Critical Infrastructure System of Systems,” *Syst. Inf. Eng. Des. Symp. (SIEDS), 2014*, vol. 00, no. c, pp. 316–321, 2014.

[60] Y. Fan, Z. Zhang, M. Trinkle, A. Dimitrovski, J. Song, and H. Li, “A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids,” *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, 2014.

[61] Y. Zhang, L. Wang, and Y. Xiang, “Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems,” *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669–683, 2015.

[62] ICS: Industrial Control Systems Security, “Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case,” *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[63] Sophos, “Un ciberataque pudo causar el último apagón en Ucrania Actualidad•Malware•malware,” *Un ciberataque pudo causar el último apagón en Ucrania Actualidad•Malware•malware*, 2016. [Online]. Available: https://news.sophos.com/es-es/2016/12/23/ciberataque-pudo-causar-ultimo-apagon-ucrania/.

[64] INCIBE, “CrashOverride: El malware para SCI ataca de nuevo,” *CrashOverride: El malware para SCI ataca de nuevo*, 2017. [Online]. Available: https://www.incibe-cert.es/blog/crashoverride-el-malware-sci-ataca-nuevo.

[65] Official website of the Department of Homeland Security, “AWARENESS BRIEFING: RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE,” *AWARENESS BRIEFING: RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE*, 2018. [Online]. Available: https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf.

[66] Official website of the Department of Homeland Security, “HIDDEN COBRA - North Korean Malicious Cyber Activity,” *HIDDEN COBRA - North Korean Malicious Cyber Activity*, 2019. [Online]. Available: https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

[67] Official website of the Department of Homeland Security, “Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors,” *Alert (TA17-293A) Advanced Persistent Threat Activity Targeting Energy and Other Critical*

Infrastructure Sectors, 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-293A.

[68] INCIBE, "Petrolera Pemex sufrió ciberataque de ransomware," 2019. [Online]. Available: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/petrolera-pemex-sufrio-ciberataque-ransomware. [Accessed: 03-Dec-2019].

[69] Xataka Corp, "Pemex niega que esté ante un 'ciberataque' aunque en redes digan lo contrario; esto es todo lo que sabemos," 2019. [Online]. Available: https://www.xataka.com.mx/seguridad/pemex-niega-que-este-ciberataque-redes-digan-contrario-esto-todo-que-sabemos . [Accessed: 03-Dec-2019].

[70] Bloomberg, "A Hacker Wants About $5 Million in Ransom From Pemex By End of November," 2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-11-13/a-hacker-wants-about-5-million-from-pemex-by-end-of-november . [Accessed: 03-Dec-2019].