IMPLEMENTACIÓN DE LA GUÍA DE CIBERSEGURIDAD DEL ACUERDO CNO 1502 EN UNA CENTRAL HIDROELÉCTRICA

Juan Pablo Gutierrez - John Jairo Copete

CELSIA COLOMBIA S.A E.S.P. Calle 15 No. 29b – 30 - Yumbo, Colombia
jpgutierrez@celsia.com - jcopete@celsia.com

RESUMEN

La ciberseguridad es una de las principales preocupaciones de las empresas de todo el mundo, además es una palabra que se ha vuelto de moda ya que la escuchamos frecuentemente en noticias relacionadas con internet, bancos, portales Web, empresas del sector salud, el gobierno, industria, ataques cibernéticos, etc. Por otro lado, este se ha convertido un tema muy complejo para todas las empresas, aparte de esto hoy en día no sabemos cómo protegernos ante un ataque cibernético. Por esta razón el sector eléctrico en Colombia en cabeza del CNO (Consejo Nacional de Operación), expidió el Acuerdo 1502 de 2021 con el cual se aprueba la guía de Ciberseguridad en todos los agentes de la cadena del suministro de energía (anteriormente 788 de 2015).

1. INTRODUCCION

El sector eléctrico en Colombia está compuesto por 4 actividades o negocios, Generación, Transmisión, Distribución y Comercialización, las cuales se rigen por las leyes 142 y 143 de 1994, en donde se define el régimen de prestación del servicio público de energía, también define las funciones de la principales entidades del sector eléctrico y su gobernanza. [1]. El CNO fue creado por la ley 143 de 1994 y su función principal es acordar los aspectos técnicos para garantizar que la operación del Sistema Interconectado Nacional (SIN) sea segura, confiable y económica y ser el ejecutor del Reglamento de Operación [2]. El 3 de septiembre de 2015, el CNO expidió el acuerdo CNO 788 con el que aprueba la Guía de Ciberseguridad, para que todos los agentes del sector eléctrico en Colombia fortalecieran sus capacidades de poder gestionar y dar respuesta frente al riesgo de ataques Cibernéticos. A su vez el acuerdo para implementar la Guía de Ciberseguridad ha pasado por varias actualizaciones, la 1241 de 2019,la 1347 de 2020, la 1463 de 2021 y la vigente 1502 de 2021, que al igual que las anteriores, será actualizada en el 2025, a la presente de la elaboración de este artículo se encuentra en revisión por parte del CNO y de los representantes de los agentes que hacen parte del comité de Ciberseguridad [3].

Por eso este trabajo se centra en el caso de éxito de la implementación de la guía de Ciberseguridad en la Central Hidroeléctrica (CH) del Alto Anchicaya, un activo crítico del SIN que cuenta con varios ciberactivos críticos entre los que tenemos Equipos Electrónicos Inteligentes (IED) de protecciones para los generadores y las líneas de transmisión, Sistemas de Control Industrial (ICS), Controladores Lógicos Programables (PLC), Gateway, que garantizan la operación confiable y que con la implementación del acuerdo se disminuye el riesgo de sufrir un ataque cibernético, lo que podría poner en peligro la seguridad de la CH y el SIN

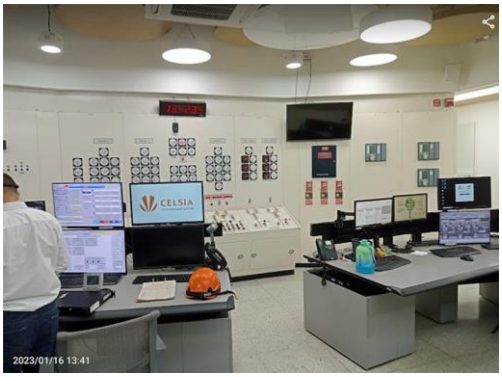

Fig. 1 Sala de Control CH Alto Anchicayá

2. PANORAMA DE LA CIBERSEGURIDAD

En 2024, se reportaron un número récord de ciberataques a nivel mundial. Se estima que hubo más de 3 millones de intentos de ciberataques diarios, Colombia experimentó un incremento significativo en los intentos de ciberataques. Según un informe de Fortinet, entre enero y noviembre del 2024 se registraron 36 mil millones de intentos de ciberataques en el país [4], algunos de estos afectando el sector eléctrico como el caso de Air-e, la principal comercializadora de energía en la región Caribe, sufrió un ciberataque el 2 de septiembre que comprometió sus sistemas informáticos, afectando a 2,35 millones de usuarios [5], XM, operador del Sistema Interconectado Nacional, reportó la neutralización de aproximadamente 9.000 ataques dirigidos a su sistema [6].


El ciberataque contra Air-e planta un nuevo obstáculo para el rescate de la energética responsable de media región Caribe

La falta de información contable complica el trabajo de interventoría para reflotar a la mayor comercializadora de la zona

Fig. 2 Ciberataque a empresa Air-e

Ahora, para entender un poco más del panorama y el impacto, los expertos afirma que los incidentes cibernéticos son la causa más temida de interrupción de los negocios, dado que solo en el 2024 los delitos cibernéticos le costaron al mundo cerca de 9,5 billones de dólares [7], estos costos incluyen daño y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción del curso normal del negocio después del ataque, investigación forense, restauración y eliminación de datos y sistemas pirateados, daño a la reputación, costos legales y, potencialmente, multas regulatorias.

Por otro lado, está el panorama del incremento de las vulnerabilidades, En 2024, se registraron un total de 40.287 vulnerabilidades, según en la base de datos de Common Vulnerabilities and Exposures (CVE) [8]. un incremento del 100,8% en comparación con 2023.

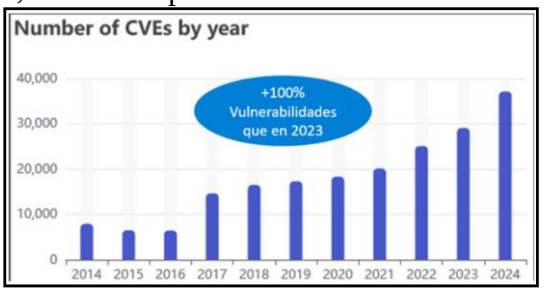

Fig. 3 Registro de vulnerabilidades reportadas por año

Este aumento equivale a un promedio de más de 100 vulnerabilidades reportadas diariamente, Una parte considerable de las vulnerabilidades reportadas por CVE afecta a sistemas de control industrial (ICS) y SCADA, se estimó que alrededor del 10-15% de las vulnerabilidades reportadas en 2024 podrían tener impacto directo o indirecto en el sector eléctrico, especialmente en componentes como sistemas de gestión de energía, software de monitoreo y dispositivos conectados.

Todo esto convierte la ciberseguridad en uno de los desafíos más crítico a nivel global,

afectando tanto a organizaciones privadas como a gobiernos y sectores clave, como el energético, financiero y de salud. Las amenazas cibernéticas son cada vez más sofisticadas, y los atacantes utilizan herramientas avanzadas, incluida la inteligencia artificial, para explotar vulnerabilidades.

Las infraestructuras críticas, como las del sector eléctrico, sanitario, y financiero, son cada vez más blanco de ataques. Esto incluye sistemas SCADA y de control industrial, esenciales en la operación de plantas de energía y redes eléctricas. El panorama de la ciberseguridad muestra una creciente sofisticación de los atacantes y una vulnerabilidad continua [9]. La adopción de nuevas tecnologías, como la IA y la computación en la nube, presenta tanto oportunidades como riesgos, lo que hace esencial fortalecer las estrategias de ciberseguridad para mitigar el impacto de los ataques.

3. ACUERDO CNO 1502

El acuerdo fue basado en las normas NERC (North American Electric Reliability Corporation) y por los estándares CIP (Critical Infrastructure Protection) [10], que es un estándar de Ciberseguridad que aplican las empresas eléctricas en EE.UU. y algunos países latinoamericanos como México, Ecuador, Brasil, Perú y Colombia. Los estándares que se usan de la norma van desde la CIP-002 a la CIP-014 y se describen a continuación:

CIP-002-5.1a Categorización de ciberactivos críticos
CIP-003-7 Gestión de controles de seguridad
CIP-004-6 Personal y entrenamiento
CIP-005-6 Perímetro(s) de seguridad electrónica
CIP-006-6 Seguridad física de ciberactivos críticos
CIP-007-6 Gestión de seguridad del sistema
CIP-008-5 Reporte de incidentes planes de respuesta
CIP-009-6 Planes de recuperación de ciberactivos críticos
CIP-010-3 Gestión de la configuración, cambios y evaluación de vulnerabilidades
CIP-011-2 Protección de la información
CIP-013-1 Ciberseguridad cadena de suministro
CIP-014-2 Seguridad física

El acuerdo incluye 2 anexos, el primero incluye los criterios para definir los activos críticos que deben ser considerados para aplicarles el acuerdo

Los siguientes son los criterios para considerar un activo critico

- Centrales de generación con capacidad efectiva neta mayor o igual 20 MW.
- Cada recurso o grupo de recursos de potencia reactiva (excepto generadores) instalados desde el Nivel IV hasta el STN.
- Todas las subestaciones con sus respectivas bahías, en aquellas subestaciones con nivel de tensión IV y superior.
- Flexible AC Transmisión Systems (FACTS) instalados en subestaciones con nivel de tensión IV y superior.
- Esquemas especiales de protección como los esquemas suplementarios, que operan de tal manera que garantizan la confiabilidad del sistema.
- Cada sistema que ejecuta desconexión automática de carga por bajo voltaje o baja frecuencia.
- Cada centro de control o centro de control de respaldo usado para ejecutar las obligaciones funcionales del operador del sistema, Generador, Transmisor o Distribuidor.
- Cualquier activo adicional que soporte la operación confiable de interconexiones internacionales.
- Cualquier activo adicional que soporte la operación confiable del SIN que la entidad

responsable estime adecuado incluir en su evaluación.

El segundo anexo trae la lista de cumplimiento periódico de la guía de ciberseguridad por cada capitulo

- Capítulo 1 Ciberseguridad introducción y Antecedentes
- Capítulo 2 Aplicación de la guía
- Capítulo 3 Cumplimiento de la guía
- Capítulo 4 Identificación de activos críticos
- Capítulo 5 Gobierno y gestión del personal
- Capítulo 6 Perímetros de seguridad
- Capítulo 7 Gestión de la seguridad
- Capítulo 8 Planes de recuperación
- Capítulo 9 Plan de respuesta ante incidentes
- Capítulo 10 Seguridad física de Ciberactivos críticos
- Capítulo 11 Gestión de la cadena de suministro

En el capítulo 4, el acuerdo pide, identificar, documentar y realizar un inventario de los ciberactivos críticos esenciales para la operación confiable de los activos críticos y para ser identificado como un ciberactivo crítico debe cumplir con al menos una de las siguientes características:

- El ciberactivo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciberactivo usa un protocolo enrutable con un centro de control, o,
- El ciberactivo es accesible por marcación.

4. ACTIVIDADES DE IMPLEMENTACIÓN

El Acuerdo CNO 1502 de 2021, adoptado por el CNO en Colombia, establece lineamientos específicos para mejorar y garantizar la operación SIN. Su implementación requiere que las empresas del sector eléctrico y los agentes involucrados en el SIN cumplan con las disposiciones estipuladas, sin embargo, su implementación, con seguridad demandara tiempo y recursos, en lo que se traduce en un costo monetario volátil, el cual es impactado por los cambios políticos. Pero el camino para las empresas del sector eléctrico es ser sostenibles y garantizar un servicio confiable y seguro, Celsia ha entendido claramente este panorama y es por ello que en este trabajo se comparte la experiencia de la implementación de la guía de ciberseguridad en la CH del Alto Anchicaya, un activo crítico estratégico para el SIN, la CH del Alto Anchicaya entró en operación en el año 1974, cuenta con tres generadores hidráulicos, los cuales tienen una capacidad de generación instalada de 355 MW, se encuentra localizada en el departamento del Valle del Cauca, 85 km al oeste de Cali en los límites de los municipios de Buenaventura y Dagua.

Fig. 4 Represa CH Alto Anchicayá

Para la implementación de los requisitos de ciberseguridad se conformó un equipo interdisciplinario donde se trabajaron en las siguientes actividades:

4.1. Actualización de políticas y notificación del responsable de ciberseguridad.

Un documento estratégico avalado y aprobado por el mayor órgano de la compañía. Esta actividad consistió en desarrollar una mesa de trabajo para la elaboración de la política que estableció todas las medidas organizativas,

técnicas, físicas y legales destinadas a la identificación, protección, detección, respuesta y recuperación de los ciberactivos críticos.
A través de este documento, se difundieron los objetivos de Ciberseguridad, de la misma forma el responsable de ciberseguridad. Todas las compañías tienen este documento, pero no todas son conscientes de su aplicabilidad, por lo que está primera actividad es crucial para el éxito de un adecuado aseguramiento.

4.2. Actualización de inventario de ciberactivos

En este punto muchas compañías se enfrentan al talón de Aquiles, un proceso que puede ser extenso y complejo, para llevar a cabo una actividad de estas, no solo se requiere de compromiso y herramientas tecnológicas, también se requiere un cambio en la cultura organizacional de la compañía, los más relevante de este proceso, fue contar con una cultura fundamentada en cuatro pilares que permitieron el buen desarrollo del recurso humano.
A nivel tecnológico se realizó el análisis para seleccionar una herramienta que no solo garantizará un descubrimiento de activos, sino que permitiera a nivel general una amplia cobertura de ciberseguridad sobre ICS y sistemas SCADA, además del soporte normativo de ciberseguridad, como NERC CIP, IEC 62443, entre otras. Como el objeto de este trabajo es compartir una experiencia de forma imparcial, no nos concentraremos en publicitar una herramienta, pero si nombraremos algunas que fueron evaluadas y que cumplían con este requerimiento, tales como:

- Tenable OT Security: Es una plataforma de seguridad diseñada para proteger entornos OT/ICS (Industrial Control Systems) contra ciber amenazas, combina capacidades de descubrimiento de activos, análisis de vulnerabilidades y detección de amenazas en un solo lugar, brindando a las organizaciones visibilidad y control sobre sus redes industriales[11].
- Nozomi Networks: Es una plataforma que combina soluciones avanzadas de ciberseguridad y monitoreo para sistemas de control industrial (ICS), sistemas SCADA y entornos de IoT. Fue diseñada para proteger redes complejas, como las utilizadas en sectores como manufactura, energía, transporte, petróleo y gas, y servicios públicos [12].

Bajo este tipo de tecnología se soportó esta activad dejando como resultado la documentación de todos los ciberactivos críticos de la central Alto Anchicaya, pero como se mencionó, el recurso humano soportado por una cultura organizacional, son garantes del desarrollo adecuado de esta activad.

4.3. Definición de los perímetros de seguridad electrónica para los ciberactivos.

Identificar y proteger los perímetros de seguridad dentro de los cuales residen los ciberactivos críticos, es el objetivo de esta actividad. Para ello se identificó un marco que permitirá la identificación de los diferentes componentes de la red y que estuviera basado en estándares internacionales, el resultado de la investigación permitió que se modelaba la arquitectura de la Central bajo el modelo SGAM (Smart Grid Architecture Model), estos marcos permiten identificar brechas, redundancias y problemas en la topología de red.

Basados en la arquitectura que fue diseñada para la central, se identificó y documento:

- El perímetro de la Central.
- Lista de acceso del personal con permiso a los ciberactivos críticos.
- Procedimiento de monitoreo de los ciberactivos críticos.
- Entre otros.

El resultado de la actividad concibió un activo crítico protegido por un perímetro de seguridad, el cual su personal solo podrá alcanzar un ciberactivo crítico estando de forma remota, si y solo si esta explícitamente permitido en las reglas del perímetro de seguridad.

4.4. Gestión de la seguridad de los ciberactivos críticos de la Central.

La operación de la central y las actividades de mantenimiento, son procesos prioritarios, es por ello que gestionar su riesgo a niveles aceptables sobre cada uno de sus ciberactivos, fue el propósito de esta actividad.
La comunicación y el entendimiento con los fabricantes es fundamental, por ejemplo el despliegue de soluciones de antimalware sobre sistemas que soportan el SCADA, es posible realizarse una vez se pueda establecer el entendimiento de la operación del antimalware y el fabricante otorgue su visto bueno, fue así que la solución del SCADA de la central logro contar con este control, también en este dominio se implementó un procedimiento para la identificación de vulnerabilidades y su proceso de parchado, todo esto gestionado y monitoreado por medio de un Centro de Operaciones de Ciberseguridad (SOC), el cual monitorea 7 x 24 la eficacia de los controles implementados.

4.5. Plan de recuperación de ciberactivos críticos.

La preparación con buenas prácticas permite tener un personal residente entrenado con habilidades para mitigar el riesgo y darle continuidad al negocio.
Este dominio permitió entender que la ejecución de ejercicios de recuperación de ciberactivos críticos establece los pilares para garantizar la continuidad del negocio en la operación de la central, no solo en momentos en que el ciberdelincuente ha tomado ventaja, sino en aquellos momentos que el ciclo de vida del ciberactivo así lo determine, por ejemplo, una falla de hardware.
Para llevar a cabo estas actividades, es necesario contar con una metodología que permita establecer las reglas que se deben aplicar para el éxito de esta tarea, entre ellas están:

- Establecer el procedimiento.
- Establecer el Plan de pruebas.
- Documentación de las pruebas realizadas.
- Entre otras.

Siguiendo esta estrategia se logró establecer para la central, las pruebas de recuperación para IED y sistemas SCADAS, generando concientización al personal en su preparación ante cualquier evento inesperado que amenace la operación de la central.

4.6. Plan de respuesta ante incidentes en ciberactivos críticos.

Al igual que del punto anterior, el éxito de garantizar la continuidad del negocio en la operación recae en lo consciente y preparado que el personal esté sobre escenarios opuestos que tenga que enfrentar en la operación normal.
En este punto toma relevancia la importancia que tiene el personal de la operación y la relación con los equipos de ciberseguridad.
Comprender la importancia de la notificación oportuna, los canales de notificación y actos sospechosos son algunos de los objetivos que se logra en el establecimiento de las pruebas ante incidentes de ciberseguridad.
Por otro lado, los equipos de ciberseguridad refuerzan o ajustan sus manuales para responder ante un incidente, esto lo logran por medio de programación de simulacros, que llevan a cada rol lo más cercano posible de un incidente de ciberseguridad.

4.7. Seguridad física de ciberactivos críticos

No solo la operación de la central se puede ver amenazada por eventos cibernéticos, también está el riesgo de actos físicos por una operación sobre un ciberactivo por un personal no autorizado, el objetivo de este dominio permitió controlar los acceso sobre un activo, que por su tamaño e importancia, tiene una gran concurrencia de contratistas y visitantes, por ello, controles como; control de acceso biométrico sobe las salas de control, cuartos CPD (Centro de procesamiento de Datos), casa de máquinas, control de visitantes, entre otros, garantizaron la adecuada administración del alcance o acceso a lo ciberactivos críticos de la central.

4.8. Gestión de la cadena de suministro.

Por ultimo y no menos importante tenemos un punto que en muchas ocasiones, se logra descuidar.

En el 2020 se presentó uno de los ciberataques con mayor impacto en la cadena de suministro, fue el ataque a SolarWinds [13]. Esta empresa que desarrolla software para la gestión de redes y sistemas, utilizado por miles de empresas y agencias gubernamentales en todo el mundo. Los atacantes comprometieron el sistema de desarrollo de SolarWinds y lograron insertar un código malicioso en las actualizaciones de su software Orion, una plataforma ampliamente usada para la monitorización de redes. Cuando las organizaciones descargaron e instalaron estas actualizaciones legítimas pero comprometidas, sin saberlo, permitieron que los atacantes accedieran a sus sistemas. Afectando a más de 18,000 organizaciones que descargaron las actualizaciones afectadas. Esto dejo como lecciones la necesidad de monitorear a los proveedores y garantizar la seguridad de sus procesos de desarrollo.

Para ello la implementación de controles que permitan la evaluación de riesgo sobre los proveedores, es una actividad periódica del equipo de seguridad, con la información de la operación de sus proveedores y fabricantes.

5. CASO DE ÉXITO IMPLEMENTACIÓN GUÍA DE CIBERSEGURIDAD

Siguiendo las buenas prácticas de la guía de Ciberseguridad, ahora la CH del Alto Anchicayá cuenta:

- Inventario actualizado de los Ciberactivos Críticos

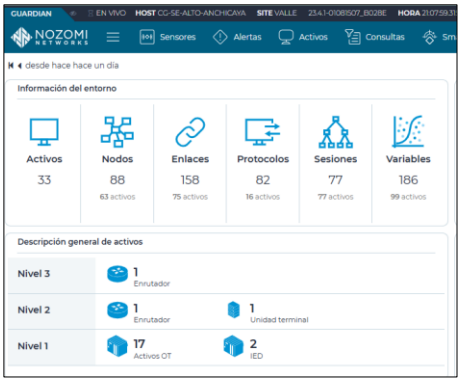

Fig. 5 Inventario activos en Nozomi

- Evaluación del estado de Ciberseguridad de la CH

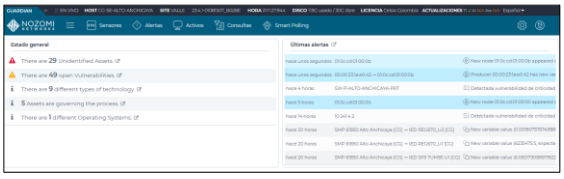

Fig. 6 Evaluación de vulnerabilidades

- Aseguramiento de los Ciberactivos Críticos mediante un perímetro de seguridad.
- Control de acceso lógico y físico a los Ciberactivos Críticos
- Gestión de vulnerabilidades

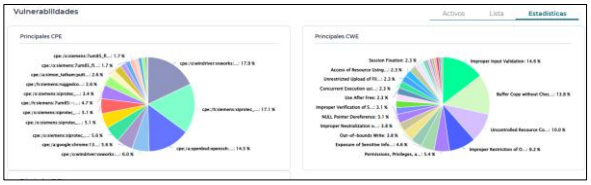

Fig. 7 Gestión de vulnerabilidades

- Ejecución de simulacros de recuperación de Ciberactivos Críticos

- Monitoreo de eventos 7/24 en la red operativa mediante el sistema de detección de intrusos

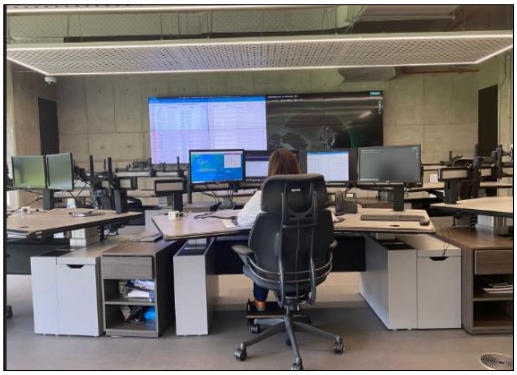

Fig. 8 Centro operaciones ciberseguridad

- Ejecución de simulacros del plan de respuesta ante incidentes de Ciberseguridad

Este conjunto de actividades nos demuestra el caso de éxito de la implementación de la Guía de Ciberseguridad del acuerdo CNO 1502 del 2021, permitiendo que la CH cuente con un buen nivel de protección de Ciberseguridad y no ver afectado su prestación del servicio de generación de energía en el SIN

6. LA GESTION DE ACTIVOS EN CIBERSEGURIDAD

La guía de ciberseguridad nace del documento CONPES 3701 del 14 de julio de 2011 en donde se establecen los lineamientos de política para la ciberseguridad y ciberdefensa, de la preocupación del riesgo de la Infraestructura Crítica Cibernética del Sector Electrico colombiano. El propósito es coordinar acciones que permitan prevenir y mitigar potenciales amenazas cibernéticas que pongan en riesgo la disponibilidad y continuidad del servicio de energía eléctrica por amenazas cibernéticas.

La gestión de activos en ciberseguridad implica administrar y monitorear los activos digitales y físicos tal como se describe en la guía de ciberseguridad y los cuales reúnen un conjunto de actividades que se describen en los capítulos del 4 al 11 del acuerdo CNO 1502

Los aspectos más destacados para la gestión de activos de ciberseguridad son:

- Contar con una política de Ciberseguridad
- Definir un responsable de Ciberseguridad
- Tener un inventario de Ciberactivos Críticos actualizado
- Contar con un programa de entrenamiento y capacitación del personal
- Tener los procedimientos de los que trata la guía
- Tener lista del personal con acceso físico a los ciberactivos críticos actualizado
- Tener sistemas de control intermedio
- Controlar las conexiones temporales de los perímetros de seguridad electrónica
- Validar los cambios realizados en los Ciberactivos críticos en las labores de mantenimiento
- Tener herramientas de prevención contra de Malware o Software malicioso
- Evaluación continua de las vulnerabilidades
- Controlar la conexión y acceso de medios extraíbles
- Actualización continua de parches de seguridad en los Ciberactivos
- Monitorear e identificar eventos de la red de tecnologías de la Operación (TO)
- Contar con un Plan de Recuperación de Desastres o PRD
- Hacer pruebas o simulacros de recuperación de Ciberactivos críticos
- Tener respaldos y almacenamiento de la información y realizar pruebas de recuperación de los respaldos
- Ejecutar un simulacro de respuesta ante incidentes en Ciberactivos Críticos
- Garantizar la seguridad física de los Ciberactivos Críticos
- Gestionar adecuadamente la cadena de suministro de Ciberactivos Críticos

La gestión de activos de ciberseguridad en los activos críticos como las centrales hidroeléctricas, no solo mejorará la seguridad;

sino que ayudará a reducir los costes a largo plazo y permitirá a las empresas responder más rápidamente a los posibles incidentes de Ciberseguridad que surjan, adicional sirve para aumentar la confianza de los clientes en la organización por tener una adecuada gestión de la ciberseguridad de sus activos

7. RECOMENDACIONES

- Contar con un gobierno de Ciberseguridad que permita la ejecución y cumplimiento de la política de Ciberseguridad
- Contar con un centro de operaciones de Ciberseguridad especializado en OT
- Establecer una cultura en situacional en Ciberseguridad entre las áreas de TI y TO
- Involucrar desde el de los proyectos tecnológicos de To al área de Ciberseguridad

8. CONCLUSIONES

- El acuerdo CNO 1502 o Guía de Ciberseguridad es una herramienta que ha permitido a las empresa que manejan la infraestructura crítica cibernética adoptar medidas y procedimiento que ayudan a mitigar los riesgos ante posibles ataque cibernéticos a los activos críticos del SIN
- Los ciberataques cada día son más sofisticados, por lo tanto, nos obliga a continuar con una gestión de activos de ciberseguridad abordando todas las recomendaciones de la guía de ciberseguridad en los agentes del sector eléctrico en Colombia
- La Guía de ciberseguridad establece una estrategia a las compañías que no solo permite ser oportunos en la identificación de brechas, sino también ser resiliente en los casos de una posible brecha.
- Establecer una cultura de conciencia cibernética, permite alcanzar a las organizaciones el nivel de madurez deseado.

BIBLIOGRAFÍA

[1] Funcionamiento del sector. (n.d.). Gov.Co. Colombia, 2025, [En línea]. Disponible en: https://www.minenergia.gov.co/es/misional/energia-electrica-2/funcionamiento-del-sector/

[2] Consejo Nacional de Operación del sector eléctrico CNO. Quienes somos. (n.d.). Org.co. Colombia, 2025, [En línea]. Disponible en: https://www.cno.org.co/content/quienes-somos

[3] Acuerdo CNO 1502 de 2021, actualización de la Guía de Ciberseguridad y se modifican algunos plazos. (n.d.). Org.co. Colombia 2025. [En línea]. Disponible en: https://www.cno.org.co/content/acuerdo-1502-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad-y-se

[4] Juan, I. D. S. (2024, diciembre 3). Colombia fue víctima de 36 mil millones de intentos de ciberataques en 2024. [En línea]. Disponible en: https://www.infobae.com/tecno/2024/12/03/colombia-fue-victima-de-36-mil-millones-de-intentos-de-ciberataques-en-2024/?utm_source=chatgpt.com

[5] Sánchez, C. (2024, octubre 24). El ciberataque contra Air-e planta un nuevo obstáculo para el rescate de la energética responsable de media región Caribe. Ediciones EL PAÍS S.L. [En línea]. Disponible en: https://elpais.com/america-colombia/2024-10-24/el-ciberataque-contra-air-e-planta-un-nuevo-obstaculo-para-el-rescate-de-la-energetica-responsable-de-media-region-caribe.html?utm_source=chatgpt.com

[6] Soler, D. M. (2024, mayo 9). Sistema eléctrico colombiano, el cuarto más vulnerable en ciberseguridad en el mundo. Portafolio. [En línea]. Disponible en:

https://www.portafolio.co/energia/ciberseguridad-sera-uno-de-los-principales-retos-para-el-sector-electrico-604458?utm_source=chatgpt.com

[7] Cybercrime Magazine. (2023, octubre 12). Cybercrime To Cost The World $9.5 trillion USD annually in 2024. Cybercrime Magazine. [En línea]. Disponible en: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

[8] Figarola, M. (2025, enero 13). Top vulnerabilidades: 2024. GitSecurit. [En línea]. Disponible en: https://www.gitsecurit.mx/2025/01/13/top-vulnerabilidades-2024/?utm_source=chatgpt.com

[9] Vulnerabilidades cibernéticas en el sector de las energías renovables en América Latina. (2024, septiembre 24). The One Brief. [En línea]. Disponible en: https://theonebrief.com/latam/post/vulnerabilidades-ciberneticas-en-el-sector-de-las-energias-renovables-en-america-latina/?utm_source=chatgpt.com

[10] NERC (North American Electric Reliability Corporation) Standards. (n.d.). Nerc.com. [En línea]. Disponible en: https://www.nerc.com/pa/Stand/Pages/Default.aspx

[11] Tenable OT Security. (n.d.). Tenable®, 2025. [En línea]. Disponible en: https://es-la.tenable.com/products/ot-security

[12] El líder en tecnología de ciberseguridad OT. (n.d.). Nozominetworks.com, 2025, [En línea]. Disponible en: https://es.nozominetworks.com/

[13] Securelist. SolarWinds: uno de los mayores ciberataques de la historia de EE.UU. roba los secretos de instituciones públicas y privadas. Kaspersky. Diciembre 28, 2020, [En línea]. Disponible en: https://securelist.lat/solarwinds-uno-de-los-mayores-ciberataques-de-la-historia-de-ee-uu-roba-los-secretos-de-instituciones-publicas-y-privadas/92142/

ACERCA DE LOS AUTORES

Gutierrez Juan Pablo, Ingeniero de sistemas de la universidad Autónoma de Colombia, Magister en Ingeniería Eléctrica, Especialista en sistemas de Transmisión y Distribución, Especialista en Automatización Industrial todos de la Universidad del Valle, Experiencia laboral en la gestión del mantenimiento de centrales hidroeléctricas por 10 años, Experiencia en la gestión, manejo configuración y pruebas de IED de protecciones en generadores hidráulicos por 7 años y Experiencia en la implementación del acuerdo CNO 1502 o Guía de Ciberseguridad en las centrales Hidroeléctricas de CELSIA Colombia

Copete John Jairo, Ingeniero informático de la Corporación Universitaria De Ciencia Y Desarrollo Uniciencia, Magister en seguridad Informática de la Universidad Internacional De La Rioja – España, con certificaciones en Incident Handler, Threat Intelligence Analyst, SOC Analyst, con más de 10 años de experiencia laboral en ciberseguridad, 5 años de experiencia en la coordinación del Centro de Operaciones de Ciberseguridad para OT de CELSIA Colombia, Docente hora catedra de pregrado de la Pontificia Universidad Javeriana Cali de la asignatura Seguridad Informática por 6 años, docente y coordinador académico del diplomado Seguridad Informatica de la Pontificia Universidad Javeriana Cali desde el año 2016.

1. Nombre del autor(es)
Juan Pablo Gutierrez – John Jairo Copete
2. Teléfono
   a. Oficina
   +57-602 3210 000
   b. Celular
   +57 316348 8247
   +57 3154568278
3. Dirección del autor(es)
   a. Oficina
   Calle 15 #29B-30 Acopi
   c. E. mail
   jpgutierrez@celsia.com
   jcopete@celsia.com
   d. Ciudad
   Yumbo, Valle del Cauca
   e. País
   Colombia