Ingeniería y Ciencia
ISSN:1794-9165 | ISSN-e: 2256-4314
ing. cienc., vol. 16, no. 32, pp. 171–194, julio-diciembre. 2020.
http://www.eafit.edu.co/ingciencia

Ciberseguridad para la operación centralizada y distribuida de generación de energía eléctrica en ISAGEN

Diego Zuluaga[1]

Recepción: 20-03-2020 | Aceptación: 04-09-2020 | En línea: 11-11-2020

doi:10.17230/ingciencia.16.32.8

Resumen

Este artículo presenta repuesta a los retos de ciberseguridad enfrentados para la centralización del control de generación de energía eléctrica en la segunda empresa de este tipo en Colombia. Así mismo, se describen las principales prácticas de ciberseguridad que se investigaron, analizaron e implementaron para establecer y mantener un entorno seguro de operaciones, que permita solucionar los riesgos de ciberataques a este servicio esencial para la sociedad; así como las metodologías y medidas técnicas que debieron tenerse en cuenta en las diferentes etapas del proyecto para evitar que los ciberataques sean efectivos, para identificarlos oportunamente y para lograr la resiliencia de los sistemas de supervisión y control que fueron empleados y probados en este entorno. También, muestra cómo estos resultados fueron usados para aportar a la evolución de la normatividad nacional en la materia y como podrán servir de base para mejoras a la regulación y la ciberseguridad de otros agentes del sector eléctrico en el país y la región.

Palabras clave: Ciberseguridad; control centralizado de energía eléctrica; ciberseguridad en generación de energía; ciberseguridad industrial; ciberseguridad de infraestructura crítica; ISO/IEC 27002.

[1] ISAGEN, dzuluagau@gmail.com, Medellín, Colombia.

Cybersecurity for Centralized and Distributed Power Generation at ISAGEN

Abstract
This paper presents the answer to the cybersecurity challenges faced by the centralization of the electric power generation control in the second company of this type in Colombia. Likewise, it describes the main cybersecurity practices that were investigated, analyzed and implemented to establish and maintain a safe environment for operations, which allow facing the risks of cyberattacks on this essential service to the society. It presents the methodologies and technical measures that should have been considered in the different stages of the project to prevent cyberattacks from being effective, to identify them in a timely manner and to achieve the resilience of the supervision and control systems that were used and tested in this environment. It also shows how these results were used as a contribution to the evolution of Colombian national electric sector regulations on the subject and how they can serve as a basis for improvements to regulation and cybersecurity for other agents in the electricity sector in the country and the region.

Keywords: Cybersecurity; centralize electric power control; power generation cybersecurity; industrial cybersecurity; critical infrastructure cybersecurity; ISO/IEC 27002.

1 Introducción

En Colombia, se maneja una frecuencia de 60 Hz en la distribución de la energía eléctrica; una desviación mayor a 0.2 Hz puede generar problemas en los procesos industriales y los equipos eléctricos. Por lo tanto, mantener el sistema con este parámetro de calidad implica un trabajo arduo para toda la cadena de generación, transmisión y distribución de energía: es necesario garantizar que la demanda y la oferta estén siempre totalmente sincronizadas y las desviaciones sean corregidas en milisegundos.

En 2015, se presentó el primer ataque a la red eléctrica de Ucrania dejando inicialmente a varias regiones sin electricidad[1] y luego, en el 2016, a su capital Kiev. El ataque, según pudieron determinar algunos investigadores que lo revisaron recientemente,

buscaba destruir equipos eléctricos[2], lo que hubiese causado efectos negativos de largo plazo para ese país. En 2018, en una alerta conjunta, el FBI[1] y el DHS[2], indicaron que el gobierno ruso estaba llevando a cabo campañas en el ciberespacio contra el sector de la energía y otros sectores críticos[3]. Así mismo, en Colombia se ha evidenciado actividad continua del grupo APT-C-36 dirigida contra empresas de infraestructura crítica en múltiples sectores. Esta actividad ha sido objeto de análisis en diferentes fuentes de ciberinteligencia tanto en 2019[4] como en 2020[5]. A partir de estos eventos, los retos de ciberseguridad en los sistemas interconectados nacionales tomaron importancia clave para la seguridad energética de las naciones.

2 La respuesta a los retos actuales de ciberseguridad para la generación eléctrica

ISAGEN, como la segunda empresa de generación eléctrica de Colombia, se ha preocupado ampliamente por alistarse y ayudar al sector y al país en su preparación frente a posibles ataques cibernéticos. Al mismo tiempo, busca desarrollar mecanismos óptimos para la operación de sus centrales de generación. Por esta razón, se emprendió el desarrollo de un Centro de Operación Integrada (COI) para sus plantas mediante el despliegue de sistemas SCADA[3] que centralizan la operación con soporte distribuido en sus centrales de generación.

El proyecto COI, actuó como catalizador y laboratorio para la implementación práctica de medidas de ciberseguridad que eran necesarias en las infraestructuras críticas de energía eléctrica, pero que eran difíciles de implementar debido principalmente a la gran

[1]FBI: *Federal Bureau of Investigation*. La principal agencia de investigación criminal de los Estados Unidos

[2]DHS: *Department of Homeland Security*. Ministerio del gobierno de los Estados Unidos que tiene por finalidad proteger el territorio estadounidense.

[3]*Supervisory Control And Data Acquisition* - Supervisión, control y adquisición de datos.

obsolescencia tecnológica, que normalmente existe en los sistemas de control industrial, y a la necesidad de mantener una operación continua e ininterrumpida con tiempos de respuesta de milisegundos para poder mantener la frecuencia del sistema dentro del rango aceptable.

El reto, entonces, consistió en establecer sistemas de control, un entorno seguro y resiliente de operaciones, y comunicaciones operativas y de gestión seguras que permitieran la operación confiable, continua y con mínimo impacto sobre la latencia para el envío de comandos de control y las recepción de las señales provenientes de los equipos de generación eléctrica.

A continuación, se recopilan las principales prácticas de ciberseguridad que se investigaron, analizaron e implementaron. Estas pueden servir de guía a diferentes empresas del sector para la implementación de sus programas de ciberseguridad industrial en proyectos similares.

3 Gobierno de la ciberseguridad y normatividad

El sector eléctrico, como Infraestructura Critica Nacional que presta el servicio esencial de energía eléctrica[6], es fundamental para el funcionamiento de nuestra sociedad actual y, más aún, del ciberespacio donde millones de personas hoy en día tienen presencia y actividades cotidianas.

Teniendo en cuenta que el ciberespacio se ha convertido en el quinto dominio de la guerra[7], el apoyo a la ciberseguridad nacional es una responsabilidad de todos los connacionales y no sólo del estado[8]; lo cual demanda el trabajo cercano y coordinado de la empresa privada con las entidades públicas y los cuerpos normativos y de control para apoyar sus iniciativas en la materia.

Es fundamental y natural para el sector eléctrico el trabajo coordinado de todos los agentes dado que si sólo uno de ellos falla, fallaría toda la cadena; no se lograría mantener la frecuencia en el nivel requerido y se comenzarían a ver los efectos en todo el país.

Adicionalmente, se haría necesaria la desconexión de algunas zonas para mantener el sistema eléctrico activo en las zonas más críticas, generando apagones en zonas menos críticas de la geografía nacional.

Esta premisa implica que el trabajo no puede ser individual de cada una de las empresas que componen el Sistema Interconectado Nacional (SIN) sino que debe ser integral con la participación de todos los agentes del sector. Un ataque, independientemente del punto de la cadena en el cual ocurra, puede afectar a todos los agentes por igual dejándolos sin producir, transmitir o distribuir la energía, generando apagones y afectando negativamente al país.

ISAGEN, y el autor de este artículo, ayudaron a que se estructuraran los planes de ciberseguridad y ciberdefensa para los sectores críticos del país mediante la participación, como socio fundador, en la Mesa de Infraestructura Crítica Cibernética del Ministerio de Defensa Nacional, liderada por el Comando Conjunto Cibernético (CCOCCI) de las Fuerzas Militares y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) adscrito al Ministerio de Defensa, a la que luego se incorporaron diversas empresas e instituciones claves para la ciberseguridad nacional.

Así mismo, con el apoyo y dirección del Consejo Nacional de Operación del sector eléctrico (CNO) y otras empresas líderes, se han mantenido esfuerzos constantes, logrando que durante el año 2019 en dicha mesa se publicara el Modelo para Agentes del Sector Eléctrico del Plan de Seguridad del Operador de Infraestructura Crítica Cibernética de Colombia[9], derivado del Plan Sectorial de Protección y Defensa para el Sector[10] que había sido publicado en el 2018 y otros documentos previamente desarrollados en conjunto.

El CNO, con participación y liderazgo de ISAGEN y otras empresas del sector, estableció desde el año 2012 una guía de ciberseguridad para los agentes del SIN, basada en los estándares NERC[4] para la protección de infraestructura crítica[11] (CIP, por sus siglas en inglés). Estos han estado en funcionamiento desde hace

[4] *NERC: North American Electric Reliability Corporation.*

más de 20 años en Estados Unidos y Canadá y llevan más de una década siendo de obligatorio cumplimiento para las empresas en esta área geográfica. Esta guía fue adoptada formalmente en el año 2015 a través del acuerdo CNO 788[12], donde además se exigieron algunos apartes mínimos de cumplimiento a los agentes del sector, se definieron los criterios para identificar los Activos Críticos del Sistema Interconectado Nacional (SIN) que podrían afectar su confiabilidad u operatividad. Se definieron los Ciberactivos como el hardware, software, información y los elementos que permiten acceder de forma local o remota; y se establecieron las medidas de protección necesarias para éstos como eje de esta normatividad.

Durante el 2019, los aprendizajes obtenidos en las implementaciones del proyecto COI, que se presentan a continuación, fueron fundamentales para liderar la discusión, construcción, publicación y acogida por parte de los agentes del sector del acuerdo CNO 1241, en el cual se establecieron las exigencias completas en materia de ciberseguridad para el sector[13]. Así mismo, sirvieron de insumo para la verificación de la factibilidad de implementación del acuerdo normativo, el cual establece la hoja de ruta de cumplimiento de ciberseguridad para todos los agentes del SIN en Colombia; durante el 2020, permitió evaluar los impactos de la pandemia en su cumplimiento, lo que ayudó a revisar los requerimientos de aplazamiento que se vieron reflejados en el nuevo acuerdo 1347 en septiembre de 2020.

La Comisión de Regulación de Energía y Gas (CREG) igualmente ha mostrado su interés en la generación de normatividad al respecto y por ello, presentó la iniciativa de establecer una estrategia integral de ciberseguridad del sector eléctrico a través de la circular 072 de 2019[14].De la misma manera, el documento Política Nacional de Confianza y Seguridad Digital CONPES 3995[15], aprobado en Julio de 2020, estableció el lineamiento para que el Departamento Administrativo de la Presidencia de la República, a través del Coordinador Nacional de Seguridad Digital con el apoyo de múltiples instituciones, implanten una ruta de acción para el desarrollo de la normatividad en materia de seguridad digital, que entre otras, tendrá

en cuenta las Tecnologías de Operación (OT por sus siglas en Inglés) como las que se aseguraron en el proyecto y se mencionan en este artículo.

4 El Método

A continuación, se describe el método utilizado para el desarrollo del Centro de Operaciones Integrado en ISAGEN.

4.1 Selección de marcos de trabajo

La definición de un marco normativo, que permitiera guiar el trabajo de gestión de riesgos de ciberseguridad para el COI, partió de la verificación de opciones disponibles en el mercado, de las tendencias naturales de este y de las señales normativas que se están dando a nivel nacional e internacional.

Estándares internacionales, como lo son el conjunto de las normas ISO 27000, son comúnmente aceptados para la seguridad de información[16]. En ISAGEN, ya se había usado el sistema de gestión ISO/IEC 27001 como base para su modelo de seguridad, lo cual era adecuado, pero se debió tener en cuenta que en sistemas de control industrial y SCADA, existen particularidades que no permiten aplicar algunos controles, y que exigen que en la triada de la seguridad[17] sea más importante la disponibilidad y la integridad, antes que la confidencialidad. Adicionalmente, se antepone la seguridad de las personas, el medio ambiente y los equipos, a la seguridad de la información misma. Esto hizo valioso ajustar elementos con el documento de referencia técnico ISO/IEC 27019 del 2017[18], que se basa en la ISO/IEC 27002, pero está enfocado en la seguridad en los sistemas de control de procesos en la industria de energía.

Adicionalmente, se consideró que el COI como infraestructura crítica cibernética debía responder a las necesidades de este tipo de sistemas, y por lo tanto, su gestión debía estar basada también en marcos de trabajo especialmente diseñados para este tipo de

infraestructura. Un ejemplo, es el Marco de Trabajo para la Ciberseguridad de NIST[19, 20] que en su núcleo, establece la necesidad de mantener las funciones de *identificar*, *proteger*, *detectar*, *responder* y *recuperar*, para una gestión efectiva de la ciberseguridad.

Figura 1: Núcleo del Marco de Trabajo del NIST. Fuente: N. Hanacek/NIST. https://www.nist.gov/cyberframework

De la misma manera, se escogió un conjunto de estándares ya probados que pudiesen ser exigibles a los fabricantes y que ya estuviesen maduros en el mercado. Así, se seleccionaron las normas NERC CIP[11] como guía para el trabajo, lo cual también se alinea con lo establecido por el Consejo Nacional de Operación y que estaban en la guía adoptada en el Acuerdo CNO 788[12], esto garantizaba su cumplimiento. Adicionalmente, se profundizó en el estudio y aplicación de las mejoras ofrecidas en las versiones más recientes de los estándares NERC CIP, que aún no eran aplicados en el país, pero que tenían un potencial importante como medidas que probablemente serían aceptables y adecuadas a la realidad nacional.

4.2 Establecimiento de requisitos de ciberseguridad en todas las fases del proyecto

Fue fundamental establecer requisitos desde un principio, cuando se realizó el diseño de la solución y se realizó la contratación de los sistemas, para lograr los objetivos de ciberseguridad. Dichos objetivos fueron la guía de implementación durante todo el proyecto, y permitieron realizar las verificaciones en cada fase de pruebas e implantación, así como identificar los avances y los resultados de las medidas de seguridad para lograr una plataforma más segura y resiliente. Los requisitos consideraron el manejo de los equipos e información de la empresa en la cadena de suministro, es decir, por el fabricante y los integradores que este subcontratase, para evitar que un tercero malintencionado pudiese incorporar elementos peligrosos en fases previas a la implementación en el sitio final. Los requisitos igualmente incluyeron la posibilidad de revisión en cada fase, para verificar que las diferentes integraciones no hubieran aumentado la exposición y que los niveles de riesgo se mantenían acotados.

5 Identificar la superficie de ataque

Es clave para la protección de la infraestructura tener claro cuáles son los Ciberactivos Críticos[5], que podrían ser susceptibles de ataque y facilitarían tomar acciones de control sobre los Activos Críticos[6] de generación[21].

Fue importante también identificar otros activos que no parecían relevantes en la operación, pero que son igualmente significativos para la transmisión de los datos, o en el esquema de riesgos de ciberseguridad, y por ende tienen que ser protegidos adecuadamente. Adicionalmente, se debieron considerar elementos que aparentemente

[5]Dispositivo para la operación confiable de activos críticos que cumple los atributos descritos en el numeral 4.2.2. de la Guia de ciberseguridad del CNO[21]

[6]Instalaciones, sistemas o equipos eléctricos que de ser destruidos, degradados o puestos indisponibles, afecten la confiablidad (suficiencia y seguridad), operatividad o que comprometan la seguridad de la operación del SIN.

son menores, como los sistemas para desplegar la medición de tiempos de GPS o las pantallas de las salas de operación que cuentan con equipos de administración y gestión basados en IP; estos equipos pueden ser susceptibles de ataque y, aunque directamente no pueden afectar la operación, pueden ser usados como punto de entrada a la red o para causar efectos no deseados en la operación.

En cuanto a la identificación de ciberactivos críticos, es fundamental obtener la información clave como el modelo, sistema operativo y versión. Esto permite no solo identificar riesgos y vulnerabilidades presentes en la plataforma, sino también contar con esta información para en el futuro, identificar vulnerabilidades que afecten el entorno de operación cuando salgan nuevas advertencias de seguridad de los diferentes fabricantes.

Por lo anterior, mantener un inventario mínimo de dispositivos, ubicación, sistema operativo y/o firmware, es básico para las tareas de gestión de seguridad.

De la misma manera, la identificación de los riesgos a los que están expuestos estos sistemas es fundamental, para lo cual se debieron tomar múltiples fuentes como los estudios internacionales y nacionales en la materia, por ejemplo el Plan Sectorial de Protección y Defensa para el Sector Electricidad de Colombia (PSPSE) [22], donde se definieron 40 riesgos cibernéticos para el sector de la electricidad que eran aplicables a este escenario y que van desde el malware hasta el sabotaje por medio electrónico, pasando entre otros por Ciberterrorismo, acceso remoto no controlado, ataques a la cadena de suministro, los dispositivos de safety y sistemas de control industrial; sumado a los ya identificados en la empresa como la obsolescencia de algunas tecnologías y la falta de estandarización de la tecnología en las diferentes centrales de generación.

6 Protección

La protección requirió actividades sobre las personas, la tecnología y los procesos. En esta sección, se presentarán algunas de las actividades que tuvieron mayor impacto en los resultados.

6.1 Canales de comunicación seguros e independientes

Para el COI, se diseñó un esquema que considera canales independientes para la gestión y la operación, permitiendo limitar el canal de operaciones al uso del protocolo Industrial IEC 60870-5-104[23]. A través de este protocolo se realiza la recepción de señales y alarmas de los equipos de generación. Con base en la información recibida, se toman decisiones para la operación y se ejecutan maniobras para llevar los equipos a condiciones seguras y óptimas. Para desarrollar este proceso sin que se presenten interrupciones o latencia en la comunicación, debido a otro tráfico, y garantizando la integridad de los comandos de control, la información de operación se envía directamente entre firewalls centrales por redes privadas virtuales (VPN). El canal de gestión, el cual permite a los mantenedores del sistema realizar procesos de configuración y administración de los equipos, se mantiene independiente del canal de comunicación industrial.

6.2 La implementación de una arquitectura de seguridad multicapa

El diseño de una arquitectura que separe las diferentes zonas de seguridad y establezca niveles de control diferentes para cada una de ellas fue considerado; las zonas de seguridad diferencian entre las labores de administración y las labores de operación. Los perímetros se definieron separando diferentes zonas, según su función y requerimientos de interconexión para permitir una operación segura y eficiente.

La operación debió ser protegida contra efectos indeseados de las medidas de seguridad, por lo que no se usaron medidas de prevención de intrusiones en comunicaciones de operación, ya que un bloqueo inadecuado de señales de supervisión o control generaría comportamientos anómalos peligrosos para la operación.

Los sistemas de firewall empleados para separar las capas de seguridad se definieron utilizando una configuración de alta

disponibilidad, y sus reglas de control de acceso se establecieron con base en la política de menor privilegio[24] según la necesidad de conexión.

6.3 Conexiones remotas seguras

Los mantenedores se conectan de manera segura usando VPNs con doble factor de autenticación. Dichas conexiones pasan a través de múltiples capas de control compuestas por diferentes niveles de filtrado con firewalls, y de monitoreo con sistemas de detección y prevención de intrusiones.

Para conexiones remotas, se establecieron mecanismos de monitoreo avanzado y grabación de sesiones, que permiten observar las actividades realizadas por el personal de mantenimiento, a la vez que genera las alertas requeridas para identificar posibles amenazas a la seguridad del sistema.

6.4 El establecimiento de líneas bases

Definir una línea base de configuración segura o estándar de seguridad para los equipos fue fundamental. Permitió establecer el estado de seguridad inicial de la plataforma, corregir errores de configuración, estandarizar y limitar la exposición a prácticas inseguras de implementación que pudieron darse en los diferentes sistemas operativos y ambientes si hubieran sido dejados como salieron de la fábrica sin revisión o adaptación a la situación normal de operación.

Estas líneas base de configuración, en un inicio, fueron definidas internamente, pero posteriormente fueron evaluadas contra buenas prácticas comúnmente aceptadas por la comunidad de seguridad. Para el proyecto COI, se emplearon las líneas de base recomendadas por el Centro para la Seguridad en Internet [25](CIS por sus siglas en inglés), ya que son las normalmente usadas por la casa matriz y son evaluables

mediante herramientas automatizadas estándar que ya venían siendo empleadas en la infraestructura de la empresa.

Las líneas bases se debieron construir para los diferentes tipos de sistemas operativos y dispositivos, con el fin de que realizaran la cobertura adecuada y, correspondieran a lo que se podía implementar y revisar en las diferentes etapas del proyecto y su posterior administración.

Estas líneas bases se diseñaron aplicando el principio del menor privilegio[24] y la disminución del panorama de exposición[26], deshabilitando o limitando los servicios no requeridos, así como estableciendo niveles y medidas de seguridad adecuados para el nivel de riesgo.

6.5 Gestión de vulnerabilidades y parches

La gestión de vulnerabilidades y parches de los sistemas permitió identificar y corregir oportunamente fallas de seguridad que se presentaban en los diferentes entornos, a través de la aplicación de parches que son liberados por los fabricantes cuando estas fallas son identificadas en sus productos.

La gestión adecuada de vulnerabilidades permitió disminuir el tiempo de exposición resultante de la existencia de las mismas. En entornos de supervisión y control, normalmente, esta gestión tiende a hacerse en periodos muy amplios, ya que el riesgo de indisponibilidad del entorno al aplicar alguna corrección o parche a las vulnerabilidades prima sobre la seguridad que la práctica ofrece.

Fue muy positivo para la gestión de vulnerabilidades contar con el uso de esquemas de calidad y entornos virtualizados, que permitieron realizar parchado seguro al posibilitar el desarrollo de pruebas antes de su aplicación definitiva y manteniendo copias de los entornos funcionales a los cuales se podía retornar de manera ágil.

La revisión periódica de las vulnerabilidades, en cada una de las diferentes fases del proyecto, permitió identificar vulnerabilidades que se presentan en los sistemas, bien sea por su configuración inicial o

por su interoperación con otros componentes, que solo se hizo evidente cuando la interoperabilidad había sido alcanzada.

Para las pruebas de vulnerabilidad se emplearon herramientas comúnmente usadas en la industria, las cuales permitieron identificar, de manera automática, las vulnerabilidades y generaron reportes. Dichos reportes fueron usados por el personal del proyecto y de seguridad para evaluar alternativas de tratamiento, algunas de estas, fueron el cerrado de puertos innecesarios y el parchado; en los casos donde no era posible realizar parchado o cierre de puertos, se restringió el acceso a los servicios vulnerables a la menor cantidad de usuarios posibles y se establecieron medidas de monitoreo especiales que permitieran identificar si estas vulnerabilidades estaban siendo explotadas.

6.6 Herramientas para la gestión del *Malware*

Se incorporaron herramientas antimalware líderes en la industria, capaces de reconocer patrones y firmas de amenazas conocidas. Además, se incorporaron herramientas tipo listas blancas de aplicación que permitieron que, luego de establecida la línea base y el software que debería correr en la máquina, no fuese posible la ejecución de otras aplicaciones por parte de los operadores, mantenedores o terceros con acceso a la plataforma; a la vez que protegía de nuevas amenazas que pudieran intentar entrar en el ambiente controlado, al no permitir su ejecución.

6.7 Protección de la dimensión humana

En este proyecto fue fundamental la gestión de la dimensión humana, para la ciberseguridad. Para el éxito del mismo fue primordial lograr que todas las personas involucradas en el proyecto entendieran las estrategias de seguridad definidas y sus razones.

Fue clave, entonces, entender que el logro de los objetivos de ciberseguridad es una responsabilidad conjunta, que debe ser

abordada en equipo entre los responsables de la seguridad, la operación, el mantenimiento, los fabricantes e implementadores. Con este equipo interdisciplinario fue posible implementar las acciones de prevención, identificar situaciones de riesgo y preparase para incidentes que pudieran ocurrir, antes de que un impacto mayor se llegara a materializar.

El desarrollo de esta dimensión se logró con apoyo de los lineamientos del modelo de cambio organizacional *ADKAR* [27] (por sus siglas en Inglés). Este modelo establece que se debe lograr una Conciencia de la necesidad del cambio y el riesgo de no hacerlo, fortaleciendo el *Deseo* de los individuos para lograr el cambio y brindando el *Conocimiento* requerido apoyando el desarrollo de las *Habilidades* y *Reforzando* los factores que sostienen el cambio. Para llevarlo a la práctica se emplearon múltiples mecanismos de los que se presentan a continuación algunos relevantes

La generación de conciencia y deseo se logró a través de estrategias de sensibilización, presentando las experiencias y problemas que han ocurrido en otros lugares. También, se analizó lo que podría ocurrir en caso de una afectación a nuestro entorno de seguridad de la operación centralizada o distribuida.

Para la gestión del conocimiento y habilidades fueron relevantes las capacitaciones sobre cómo prevenir eventos de ciberseguridad, cómo tratar las alertas y cuándo escalarlas, de ser necesario.

Adicionalmente, se reforzó realizando ejercicios reales de simulación que mostraron los niveles a los que podría llegar un atacante y los impactos que esto podría traer para las operaciones de la empresa. Además, en esta fase se reforzó la conciencia a la vez que se identificaron elementos requeridos en procedimientos y procesos de operación y mantenimiento, para la atención de un incidente de ciberseguridad.

6.8 Implementación de medidas de seguridad física

La seguridad lógica es importante para la ciberseguridad, pero también es fundamental evitar el acceso físico no controlado a áreas donde se puedan encontrar Ciberactivos Críticos[28]. Estos accesos físicos restringidos tienen por objetivo evitar afectaciones al sistema de operación y su disponibilidad desde la capa física. Para ello, se debieron tomar medidas como controles de acceso tipo exclusa y con control de acceso por tarjeta y biométrico a áreas con Ciberactivos Críticos sensibles. Igualmente, se debieron considerar controles de separación de paredes dentro del centro de cómputo, de tal forma, que una persona que vaya a realizar acciones sobre sistemas administrativos no pueda intervenir los sistemas SCADA, evitando problemas accidentales o malintencionados.

Adicionalmente, se implementó el monitoreo a través de cámaras de seguridad de los espacios donde se encuentran los ciberactivos críticos. Esto permite identificar y analizar tanto eventos fortuitos como intentos malintencionados y actos contra infraestructura física, especialmente de personal que tiene acceso a estas áreas sin acompañamiento.

7 Monitoreo profundo, detección y gestión de incidentes

En las teorías actuales de ciberseguridad no basta con la prevención[29], es necesaria la detección de actividades maliciosas, el análisis y correlación de los eventos de seguridad que se presentan en las plataformas y la respuesta sobre las alertas.

En entornos industriales y de sistemas SCADA, este análisis debe garantizar que no afecta el flujo normal de los datos de supervisión y control. Por esta razón, se implementaron un conjunto de sondas de monitoreo que observan y analizan a profundidad el tráfico de red, encontrando anomalías y generando alertas. Dichas alertas son gestionadas en un centro de operaciones de seguridad (SOC por sus siglas en inglés) que opera 7x24x365 desde diferentes ubicaciones geográficas en el mundo, con apoyo del personal de operación y

mantenimiento de las diferentes plantas de generación, y el COI, lo cual requirió una gestión de cambio en el personal y en las formas típicas de operación de este tipo de sistemas.

El monitoreo, inspección profunda y correlación de paquetes en el SOC, realizado a través de las sondas, posibilitó la identificación de anomalías en las comunicaciones, comunicaciones no habituales, conexiones de equipos no autorizados, desviaciones de las líneas base y accesos a los dispositivos, de manera que el personal del SOC puede verificar con el personal responsable de la operación o mantenimiento qué está pasando.

Además, por tratarse de una infraestructura crítica nacional, se ha mantenido el monitoreo de los perímetros externos de las zonas SCADA y un trabajo conjunto para la gestión de Incidentes con el Comando Conjunto Cibernético de las Fuerzas Militares, quienes correlacionan los eventos con los de otras infraestructuras pudiendo identificar ataques de mayor envergadura.

Se mantiene, además, el monitoreo de ciberinteligencia en fuentes abiertas para identificar nuevas técnicas, tácticas y procedimientos (TTPs) empleados por los atacantes. Con estas nuevas TTP se implementan indicadores de compromiso en los sistemas de control y monitoreo, que permiten identificar y contener ataques que se puedan estar presentando en la infraestructura.

8 Continuidad, resiliencia y recuperación

8.1 Redundancia de componentes de operación y seguridad

Todo el diseño se realizó considerando que el COI actuaría como controlador de infraestructura crítica y por ende requería los más altos niveles de disponibilidad y resiliencia ante fallas. Con base en esto, la infraestructura se diseñó para lograr una operación con niveles de disponibilidad superior al 99.95 %. Esto fue posible a través de la implementación de componentes en alta disponibilidad en toda la plataforma operativa y de seguridad, así como de la verificación de los tiempos medios entre fallas de los componentes empleados.

Para la infraestructura de servidores se implementaron ambientes virtualizados en servidores hiperconvergentes en alta disponibilidad. Esta solución permitió realizar mantenimientos de hardware en tiempo real sin afectar la operación, gracias a la posibilidad de reasignación de hardware. También, fue posible realizar respaldos de la plataforma sin indisponer el sistema SCADA, con menores tiempos de ejecución de los mismos y facilitando la recuperación en caso de ser requerida.

8.2 Respaldo en operación distribuida

Desde su diseño el COI se concibió para operar de manera distribuida, permitiendo ejecutar las maniobras de control tanto desde el sitio central como desde las mismas plantas de generación, por periodos de tiempo prolongados. De esta manera, se garantiza la resiliencia del sistema en caso de eventos que afectaran la disponibilidad del mismo, o incluso de ciberataques que pudieran requerir labores de investigación forense antes de comenzar los protocolos de recuperación.

9 Resultados y discusión

Al aplicar las medidas de ciberseguridad en este entorno de desarrollo tecnológico se redujeron los riesgos de ciberseguridad encontrados a niveles aceptables para la empresa con los controles descritos en este artículo sobre los sistemas intervenidos,incluso, ha permitido que las vulnerabilidades críticas en los sistemas SCADA implementados se hayan reducido a cero, a través de la eliminación, corrección o filtrado de las mismas,lo cual era improbable en los ambientes que comúnmente se empleaban en este tipo de infraestructura, y que en muchos casos ya eran obsoletos y sin posibilidades de implementar parches o medidas de seguridad con soportes del fabricante.

Se logró mantener la disponibilidad de la operación por encima de los niveles requeridos.

Se pudieron mantener comunicaciones seguras para la operación y gestión, sin inversiones adicionales importantes y sin aumento de latencia significativa para la supervisión y control de los equipos, permitiendo una operación remota confiable y segura de las centrales de generación.

La implementación permitió probar en el país medidas de seguridad relevantes, las cuales fueron recomendadas para la actualización de las guías de ciberseguridad. Estas guías fueron exigidas como de obligatorio cumplimiento para todo el sector eléctrico, con la certeza razonable de que será posible su implementación por los agentes del sector. Se logró igualmente mejorar el conocimiento y comportamiento de los trabajadores relacionados con la operación de las centrales de generación.

Durante el 2019, se logró la gestión adecuada de más de 1000 eventos y alertas de ciberseguridad, los cuales fueron identificados a través del monitoreo en tiempo real y a profundidad; este monitoreo identifica, entre otros, conexiones de gestión que se verifican con los usuarios que las han realizado para confirmar su veracidad. Esto ha evidenciado la eficiencia del sistema de monitoreo y gestión de ciberseguridad. A pesar de la cantidad de eventos y alertas generadas en 2019, no se presentó ningún efecto adverso o incidente de ciberseguridad que afectara la plataforma relacionada con las tecnologías de operación del COI y las centrales involucradas en el proyecto. Se logró la implementación de tecnología robusta y actual de operación que sigue líneas bases de seguridad con lo que se ha logrado el endurecimiento de la tecnología frente a posibles ciberataques.

Un resumen de los resultados claves se presenta en la tabla a continuación:

Tabla 1: Impactos de las medidas de ciberseguridad establecidas

Función NIST	**Situación anterior**	**Situación actual**
Identificar	Indagaciones por cada vulnerabilidad a las diferentes centrales de generación para identificar dispositivos a los cuales les aplica.	De manera centralizada se puede identificar en dónde una nueva vulnerabilidad aplica y reaccionar oportunamente.

Proteger	Se convive con vulnerabilidades y tecnología obsoleta dentro de perímetros de seguridad, con sistemas no estándar de diferentes marcas y tecnologías.	Se eliminaron y/o controlaron la totalidad de las vulnerabilidades relevantes identificadas en el entorno.Se estableció la arquitectura y accesos seguros.Se establecieron líneas base seguras.Se establecieron mecanismos para la administración segura.
Detectar	Se detectan anomalías básicas.	Se pueden identificar accesos a los dispositivos y se verifican con el personal responsable del ciberactivo. Se hace inspección profunda de paquetes para identificar anomalías en las comunicaciones, comunicaciones no habituales y desviaciones a las líneas base.Se pueden identificar conexiones no autorizadas dentro de la red SCADA.
Responder	Los protocolos de respuesta debían integrar de manera ad hoc a las personas con experiencia en la operación, según el tipo de incidente que se presentara.	Se cuenta con un protocolo estandarizado de respuesta ante eventos, alertas e incidentes de ciberseguridad.El personal de ciberseguridad trabaja en conjunto con el personal de operación para clarificar los eventos y la respuesta requerida.
Recuperar	La recuperación requiere infraestructura física y con altos tiempos de restauración.	Se cuenta con ambientes distribuidos y virtualizados, infraestructura de alta disponibilidad y respaldos de la infraestructura, que permiten resiliencia y recuperación en casos de incidentes menores y mayores que puedan ocurrir.

10 Conclusiones

Con la aplicación de la tecnología actual, adaptada a las necesidades del entorno nacional, fue posible establecer un entorno ciberseguro para sistemas de control industrial y SCADA de generación eléctrica. Esto permitió la centralización de operaciones en un ambiente confiable, el cual mantiene la disponibilidad esperada y cuenta con resiliencia para fallas y ciberataques contra la operación reduciendo los riesgos a niveles aceptables, y brindando las bases para seguir evolucionando continuamente y mantener un entorno de operaciones seguro en un contexto de amenazas crecientes.

Las tecnologías de ciberseguridad que se emplearon no generaron interrupciones ni latencias perjudiciales para la operación centralizada y remota de las centrales, por lo cual pudieron ser usadas sin riesgo en este entorno de infraestructura crítica.

Se vislumbra en el futuro la aplicación de medidas similares a las presentadas en este artículo para la protección de infraestructuras críticas del sector de la energía en el país, la región y el mundo. Esto permite proveer entornos cada vez más seguros y resilientes frente a posibles ataques cibernéticos que se puedan presentar.

Resta por explorar, en futuros estudios, técnicas avanzadas de respuesta automática inteligente que puedan operar en entornos industriales, sin poner en riesgo la operación de los sistemas.

Medidas de seguridad, como las presentadas en este artículo, serán cada vez más adoptadas y exigidas por los diferentes gobiernos para garantizar la prestación del servicio esencial de energía eléctrica.

Agradecimientos

El autor agradece a ISAGEN y MINCIENCIA por el apoyo a esta iniciativa de ciberseguridad en la operación. Así mismo, agradece a Jhon Bolivar, Claudia Sandoval, Yamina Paez y especialmente al PhD. Juan Guillermo Lalinde por sus aportes en la revisión de este artículo.

Referencias

[1] R. M. Lee, Michael J. Assante, and Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Industrial Control Systems - E-ISAC, Tech. Rep., 2016. 172

[2] J. Slowik, "Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack," Dragos Inc., Tech. Rep., 2019. https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf 173

[3] CISA, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A 173

[4] Qi'anxin Threat Intelligence Center, "APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations," 2019. 173

[5] Lab52, "APT-C-36 recent activity analysis," 2020. https://lab52.io/blog/apt-c-36-recent-activity-analysis/ 173

[6] El Congreso de Colombia, "LEY 143 DE 1994," http://www.secretariasenado.gov.co/senado/basedoc/ley_0143_1994.html, 1994. 174

[7] J. Andress and S. Winterfeld, *Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners*. Syngress; 2 edition, 2011. 174

[8] A. D. Campen, "Uncommon Means for the Common Defens," in *Cyberwar: Strategy and Conflict in the Information Age*, A. D. Campen, D. H. Dearth, and R. T. Goodden, Eds. Fairfax, Virginia: AFCEA International Press, 1996, pp. 71–75. 174

[9] Ministerio de Energía and Ministerio de Defensa Nacional, "Plan de Seguridad del Operador de Infraestructura Crítica Cibernética de Colombia (Modelo para Agentes del Sector Eléctrico) PSICCN V1.0." Bogota, 2018. 175

[10] Consejo Nacional de Operación and Ministerio de Defensa Nacional, "Plan Sectorial de Protección y Defensa para el Sector Electricidad de Colombia PSPSE V1.0." Bogotá, Tech. Rep., 2018. 175

[11] NERC, "Standards," 2020. https://www.nerc.com/pa/Stand/Pages/default.aspx 175, 178

[12] Consejo Nacional de Operación, "Acuerdo No. 788 Por el cual se aprueba la Guía de Ciberseguridad," https://www.cno.org.co/content/acuerdo-788, p. 21, 2015. https://www.cno.org.co/content/acuerdo-788 176, 178

[13] Consejo Nacional de Operaciones, "Acuerdo 1241 Por el cual se aprueba la modificación de la Guía de Ciberseguridad," https://www.cno.org.co/node/86426, pp. 5–7, 2019. https://www.cno.org.co/node/86426 176

[14] Comisión de Regulación de Energía y Gas, "CIRCULAR No. 072," 2019. 176

[15] Departamento Nacional de Planeación, Consejo Nacional de Política Ecónomica y Social, "CONPES 3995," 2020. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf 176

[16] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, no. 4, pp. 92–100, 2013. http://dx.doi.org/10.4236/jis.2013.42011 177

[17] D. Denning, *Information Warfare and Security.* Addison-Wesley Professional; 1 edition, 1999. 177

[18] ISO, "Information technology — Security techniques — Information security controls for the energy utility industry," *ISO/IEC 27019:2017*, 2017. https://www.iso.org/standard/68091.html 177

[19] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, NIST, Tech. Rep., 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf 178

[20] ——, "Marco para la mejora de la seguridad cibernética en infraestructuras críticas," NIST, Tech. Rep., 2018. https://doi.org/10.6028/NIST.CSWP.04162018 178

[21] Consejo Nacional de Operación, "Guía de Ciberseguridad," Consejo Nacional de Operación, Bogota, Tech. Rep., 2019. https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/anexoacuerdo1241.pdf 179

[22] Ministerio de la Defensa Nacional, Consejo Nacional de Operación, "Plan Sectorial de Protección y Defensa para el Sector Electricidad de Colombia ," Tech. Rep., 2018. 180

[23] Y. ZHAO and Z.-j. SHEN, "Application of tcp/ip based iec60870-5-104 telecontrol protocol in power system [j]," *Power System Technology*, vol. 10, p. 016, 2003. 181

[24] F. B. Schneider, "Least privilege and more," *IEEE Security and Privacy*, vol. 1, no. 5, pp. 55–59, 2003. https://doi.org/10.1109/MSECP.2003.1236236 182, 183

[25] Center for Internet Security, "CIS - Center for Internet Security," https://www.cisecurity.org/, 2020. https://www.cno.org.co/node/86426 182

[26] D. Colesniuc and I. Martin, "Cybersecurity by Minimizing Attack Surfaces," in *International Scientific Conference "Strategies XXI", Suppl. Suppl_ Command and Staff Faculty.* Bucharest: Natinoal Defense University, 2015, pp. 42–48. https://search.proquest.com/docview/1747378360 183

[27] J. M. Hiatt, "ADKAR: a model for change in business, government and our community." Prosci Research, 2006, ch. 1, pp. 2–3. 185

[28] P. Bowen, J. Hash, and M. Wilson, "Information security handbook: A guide for managers," in *NIST Special Publication 800-100, National Institute of Standards And Technology*, 2007, pp. 178–800. 186

[29] M. Xue, S. Roy, Y. Wan, and S. K. Das, "Security and Vulnerability of Cyber-Physical Infrascture Networks: A Control-Theoretic Approach," in *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundations and Challenges*, S. K. Das, K. Kant, and N. Zhang, Eds. Morgan Kaufmann, 2012, ch. 1, pp. 5–30. 186