Comité de Estúdios D2 - Sistemas de información, telecomunicación y ciberseguridad

Evaluación de Sistemas IPS en la Prevención de Ataques Cibernéticos en Subestaciones Digitales: Validación y Análisis en un ambiente de simulación en Tiempo Real

J. OSPINA*
Kinnesis Solutions
Colombia
jeospina@kinnesis.com

L. ISAZA-GIRALDO
Kinnesis Solutions
Colombia
lisaza@kinnesis.com

D.A. PÉREZ
Kinnesis Solutions
Colombia
dperez@kinnesis.com

B.A. POTOSÍ
Kinnesis Solutions
Colombia
bapotosi@kinnesis.com

B.A. ARBOLEDA
XM
Colombia
barboleda@xm.com.co

Resumen *– Debido a la creciente integración entre las tecnologías TI (tecnologías de la información) y TO (tecnologías de la operación), ha aumentado la vulnerabilidad a las ciberamenazas en infraestructuras críticas y, particularmente, en las subestaciones eléctricas. Esta situación exige un paso extra en cuanto a medidas de seguridad. El presente artículo aborda los beneficios de los sistemas de prevención de intrusiones (IPS) en redes TO, analizando su desempeño en un ambiente de pruebas controlado. Se detallan los desafíos técnicos y las limitaciones que se podrían presentar a la hora de la implementación y, posteriormente, se discuten las condiciones y estrategias que permitirían ofrecer un panorama completo que aporte al robustecimiento de la seguridad de las subestaciones.*

Palabras clave: **Operación – Información – Subestaciones – Infraestructura – Ciberseguridad – Sistemas – Prevención – Deteción – Intrusiones - IPS**

1 INTRODUCCIÓN

La infraestructura critica se define como aquella infraestructura tan vital que su destrucción o inhabilitación tendría un efecto debilitante para la defensa o seguridad económica de un país, dentro de esta infraestructura se encuentra el sistema eléctrico de un país, y dentro de este sistema se encuentran los activos que llevan a cabo las funciones de operación principales [1]. En el caso particular de la energía eléctrica, la infraestructura se compone tanto de un componente TI (tecnologías de la información) como de un componente OT (tecnologías de la operación). Estos componentes se encargan respectivamente del manejo de todos los datos e información de las redes de comunicaciones digitales, y de gestionar a nivel físico los distintos procesos de operación [2].

Sin embargo, a pesar de que en un inicio ambos componentes estuvieran aislados, cada vez más se ve una convergencia entre estos dos mundos, la cual revela una vulnerabilidad técnica en los equipos de operación de las redes eléctricas, ya que estos son elementos con largos ciclos de vida y conforme transcurre el tiempo, se incrementa el número de amenazas cibernéticas a las que estos dispositivos podrían estar expuestos [3]. La gravedad de estas amenazas reside en la especificidad de los ataques y amenazas que se generan desde distintos ámbitos, ya que pueden ser potencialmente catastróficas para los equipos del sector [4] y, por lo tanto, para todo el sistema eléctrico del país.

Se hace entonces necesario contar con equipos como los *sistemas de detección de intrusiones* (IDS por sus siglas en inglés), quienes se dedican a analizar el tráfico de las subestaciones de forma no invasiva, o los

* jeospina@kinnesis.com, Medellín, Cra 25# 1A Sur 155 Oficina 1453

sistemas de prevención de intrusiones (IPS por sus siglas en inglés) quienes podrían llegar a bloquear tráfico malicioso incidiendo directamente en las comunicaciones de la subestación [5], ya que en el aseguramiento de infraestructura crítica, comúnmente no es posible alcanzar los objetivos de seguridad a través de la aplicación de una sola contramedida o técnica, por lo cual, estándares de ciberseguridad para el sector industrial como la ISA/IEC 62443 1-1, plantean el uso de la estrategia de defensa-en-profundidad, basada en el principio de utilizar múltiples contramedidas de seguridad de manera escalonada o en capas [6].

De acuerdo con lo anterior, la respuesta de un IDS, que se enfoca principalmente en identificar los ataques, no puede tomarse como una política de seguridad robusta por sí misma, y se ha evidenciado que la seguridad de la infraestructura crítica podría verse beneficiada por el respaldo de un IPS [7].

Este artículo se enfoca en identificar posibles inconvenientes y limitaciones a nivel técnico en la integración de estas soluciones de ciberseguridad, particularmente de los IPS, identificando posibles vulnerabilidades, proporcionando recomendaciones y estrategias que puedan facilitar el uso de estos equipos para su óptima implementación en subestaciones, garantizando la seguridad de las redes de subestaciones eléctricas y mejorando la resiliencia ante ciberataques. Este enfoque proactivo en la ciberseguridad es fundamental en un mundo cada vez más digitalizado y con amenazas cibernéticas en constante evolución, asegurando así la continuidad y confiabilidad del suministro eléctrico.

En la sección de materiales y métodos se detallan los dispositivos y las tecnologías utilizadas, así como el entorno experimental y de pruebas, posteriormente en la sección de resultados puede observarse el comportamiento del IPS al ser sometido a las pruebas descritas en la sección anterior, en la sección de discusión se abordan la costo efectividad del sistema y por último en la sección de conclusiones(..)

2 MATERIALES Y MÉTODOS

2.1 Descripción de los dispositivos y tecnologías utilizadas

Para la elaboración de las pruebas, con el objetivo de identificar posibles inconvenientes y limitaciones a nivel técnico en la integración de un IPS en un entorno de subestación simulado en laboratorio, se utilizaron los siguientes equipos:

- IPS (Intrusion Prevention System): Herramienta de seguridad de red con las mismas funciones de detección de amenazas que un IDS, pero con capacidades de prevención para bloquear directamente el tráfico malicioso de la red.
- IEDs (Intelligent Electronic Devices): Dispositivo electrónico inteligente que puede programarse para recoger datos, procesar estos datos y tomar las medidas adecuadas, comúnmente utilizado en la automatización industrial y en las protecciones del sector eléctrico.
- Switches: Dispositivos utilizados en la red con alta disponibilidad de puertos utilizados para interconectar varios equipos permitiendo que se comuniquen entre sí y compartan información dentro de una red LAN.
- DoS (Denial of Service): Ataque orientado a interrumpir el servicio de un sistema o red, al enviar un flujo de tráfico de gran magnitud proveniente de un solo dispositivo, lo cual consume los recursos de la víctima de modo que la capacidad de respuesta se vea disminuida al punto de que comience a rechazar peticiones legítimas.
- Ping: Herramienta de línea de comando que mide la latencia que existe entre la conexión de dos dispositivos de red.

2.2 Entorno experimental

Se diseñó y se implementó una arquitectura de red para una subestación eléctrica con equipos reales interconectados e instalados en un mismo rack. Dichos equipos, se integraron a un entorno de pruebas controladas utilizando protocolos según el estándar IEC61850 ya con esto se instaló dentro de la red un equipo

de ciberseguridad IPS de forma estratégica para facilitar la detección y contención de ataques malintencionados. Con el entorno experimental listo se procedió a configurar el equipo IPS de acuerdo a las necesidades de la prueba las cuales consistían en proteger las vulnerabilidades del equipo IED de un ciberataque.

El IPS trae dos modos de protección, modo Offline y modo Online, para estas pruebas es estrictamente necesario utilizarlo en modo Online de tal forma que todo el tráfico de red que llega al equipo víctima, en este caso el IED pase a través del IPS (ver Fig. 1) y de esta manera de acuerdo al perfil, políticas y reglas que se habiliten en el IPS, este pueda contener el ciberataque.

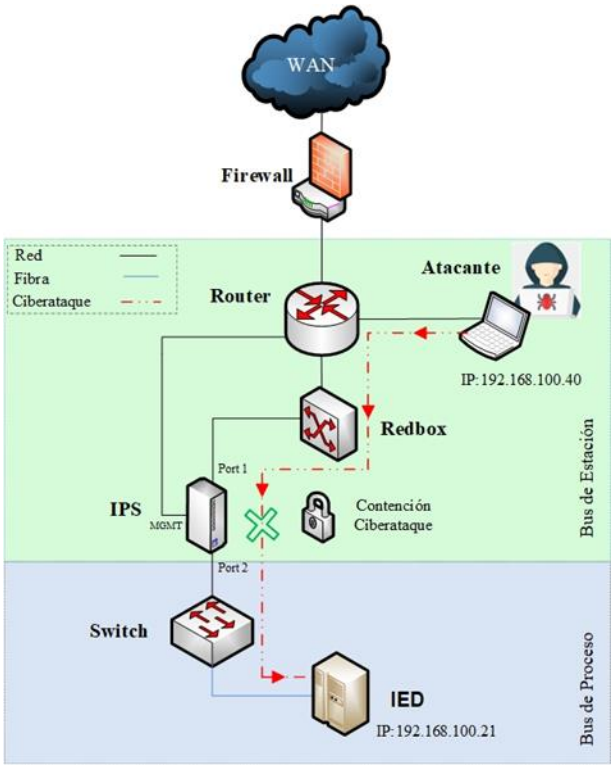

Fig 1. Esquemático de la red de la subestación simulada.

Para que el IPS contenga el ataque es importante realizar una adecuada configuración de políticas y reglas que no afecten el tráfico de red necesario para el normal funcionamiento del equipo IED, para esto se definen perfiles como el IEC61850 que utiliza protocolos *Generic Object Oriented Substation Events* (GOOSE por sus siglas en ingles), *Manufacturing Message Specification* (MMS por sus siglas en ingles) y *Sampled Values* (SV por sus siglas en ingles) que son propios del sector eléctrico, después se configuran reglas que ayuden a identificar qué tipo de tráfico de red es seguro, para esto el IPS trae un modo de autoaprendizaje que se programa por un periodo de tiempo determinado y durante este modo es capaz de crear sus propias reglas conforme al tráfico que analiza en la red, en este proceso es responsabilidad del usuario validar cuáles reglas no son adecuadas y eliminarlas para no causar un bloqueo innecesario en la operación del IED y si es necesario adicionar reglas personalizadas. Una vez creado el perfil y las reglas, se configuran las políticas de seguridad enfocadas especialmente para contener ataques de tipo DoS.

2.3 Escenarios de simulación: Ataques cibernéticos DoS y respuestas de los sistemas

Asumiendo que una persona malintencionada identifica las vulnerabilidades de los equipos IED instalados en la red de la subestación y logra tener acceso a esta para ejecutar un ataque DoS, este ataque tiene como objetivo enviar una gran cantidad de solicitudes o datos que sobrecarga el equipo dejándolo inaccesible a quienes lo necesitan legítimamente. Para validar la efectividad de implementar un IPS en una red OT se contemplan dos escenarios, el primero es cuando la red no tiene un esquema de protección de ciberseguridad implementada y el segundo cuando si se implementa protección a la red con un equipo IPS.

3 RESULTADOS

3.1 Evaluación del desempeño del IPS frente a ataques simulados

Para entender la efectividad de un IPS ante un ataque, se realiza el envío de un ping sostenido a la dirección IP del IED y se monitorea la latencia y pérdida de paquetes. Paralelamente, se inspecciona la disponibilidad y tiempo de respuesta de la interfaz web, accesible a través del puerto 4443 del IED. El objetivo de esta prueba es determinar si el ataque logra detener el servicio, observando pérdida de paquetes o indisponibilidad del servicio web.

3.1.1 Escenario 1 sin esquema de protección.

Para el primer escenario se ejecutó el ataque DoS sin la implementación de un equipo IPS o configurado de forma pasiva en modo monitoreo de red. Como resultado se observa perdida de paquetes evidenciando problemas de comunicación del IED en la red, causando graves afectaciones en la subestación (ver Fig.2)

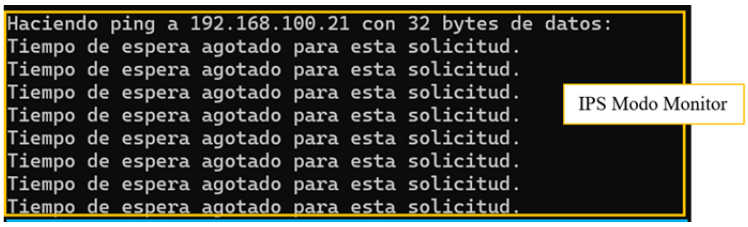

Fig 2. Perdida de latencia en la comunicación con el IED.

3.1.2 Escenario 2 con esquema de protección.

Para el segundo escenario se ejecuta el ataque DoS cuando se tiene implementado un IPS y está configurado en modo prevención con las reglas y perfiles configuradas previamente para proteger las vulnerabilidades del equipo victima o IED. Para este caso se observa que durante el tiempo que duro el ataque el IED nunca perdió comunicación en la red y trabajo en completa normalidad (ver Fig. 3) demostrando que el IPS fue capaz de contener el ataque e identificar qué tipo de ataque era, desde donde se realizó y cuál era el equipo victima (ver Fig. 4)

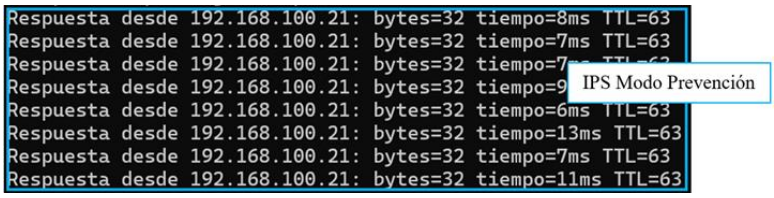

Fig 3. Comunicación con el IED sin perdidas de latencia.

Time	Function Type	Protocol Layer	Security Category	Security Severity	Security Rule Name	Interface	Attacker	Victim
2025-01-22T17:15:34-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:29-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:24-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:19-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:14-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:09-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21
2025-01-22T17:15:04-05:00	Cyber Security	Layer3	Flooding & Scan	High	TCP SYN Flood	PORT1	192.168.100.40	192.168.100.21

Fig 4. Registro de eventos del IPS durante el ataque.

4 DISCUSIÓN

Un aspecto clave identificado en esta investigación es la necesidad de que el personal a cargo del IPS deba contar con conocimiento especializado tanto en las interacciones y operación de los protocolos que utilizan los dispositivos de la subestación (MMS, GOOSE, IEC 60870-5-101, IEC 60870-5-104, DNP3, Modbus, etc.), así como la operación y parametrización del IPS, con el objetivo de permitir un correcto afinamiento en las acciones de detección y contención, minimizando eventos de falsos positivos, como bloqueos innecesarios de tráficos en IEDs en la subestación. Si bien esto puede ser complejo encontrar en un solo perfil dentro de las organizaciones, se vuelve necesario el trabajo conjunto y complementario entre el personal de operación con el equipo de ciberseguridad.

Lo anterior describe el desafío principal a la hora de implementar un IPS en un entorno de subestación y también en el entorno industrial: el bloqueo de tráficos en OT en la etapa de producción. Evaluar en entorno de laboratorio la operación de un IPS se vuelve obligatorio para poder identificar previamente los diferentes protocolos y comunicaciones del proceso, así como las distintas funciones y soporte de protocolos OT que la solución IPS ofrezca, si es enfocado para subestaciones o para entornos industriales. Esto se puede observar en estudios previos [8] en los cuales se valida la existencia de múltiples soluciones IPS para la industria, además de ayudar a visualizar como estrategia para su parametrización, una etapa previa de monitoreo de tráficos en modo pasivo o de detección como IDS antes de operarlo en modo activo como IPS.

Los resultados de la presente investigación permiten tener una aproximación inicial al escenario de la implementación de un tipo de solución tecnológica activa tipo IPS, la cual permite apoyar los análisis que las empresas del sector eléctrico a nivel Iberoamérica pueden optar frente a la creciente digitalización de las subestaciones eléctricas así como en la sofisticación de las amenazas cibernéticas que pueden estar expuestas, sin embargo, la implementación de una solución de monitoreo o prevención de eventos de ciberseguridad deberá ser el resultado de la aplicación de estándares o regulaciones, políticas y un análisis de riesgos para determinar su viabilidad técnica y económica.

El análisis de costo-beneficio de una solución de ciberseguridad es un factor importante y complejo para considerar su implementación, ya que requiere de evaluaciones de riesgos, vulnerabilidades, cumplimiento de estándares, cultura organizacional, acompañado de métricas para su medida [9], la cuantificación de los costos directos de su adquisición, implementación y mantenimiento, así como el dimensionamiento de los costos que pudieran derivarse frente a la ocurrencia de un evento como el apagón de una subestación, además de la pérdida de reputación en caso de que el incidente no pueda ser prevenido o contenido

Para el caso de la implementación de una solución tipo IPS, un punto de partida para poder realizar dicho análisis es conocer su costo en el mercado, que depende de los componentes dimensionados para su operación (hardware, software, plataforma de gestión, etc.) al que debe agregarse el costo de los servicios de implementación. La cuantificación total del costo-beneficio requerirá de la aplicación y análisis detallado de los anteriores factores enunciados entendiendo la situación operacional de cada caso.

Informes recientes realizados por líderes en soluciones de ciberseguridad han revelado que sectores de infraestructura crítica como energía, oil/gas han sufrido ataques de ransomware, principalmente debido a explotación de vulnerabilidades (49%), sugiriendo priorizar la implementación de parches basado en un análisis de riesgos. Dichos ataques han demandado pagos de rescate entre USD$1M y USD$5M en el 71% de los casos, así como costos de recuperación de USD$3.12M en promedio en el 2024 [10]. La solución IPS con funciones de parcheo virtual para equipos legacy, ofrece una alternativa de solución para prevenir y contener la explotación de vulnerabilidades en los casos donde ya no es posible realizar el parcheo.

5 CONCLUSIONES

La implementación de un IPS en subestaciones, mejora la seguridad y disponibilidad de las redes OT, siempre y cuando éste esté configurado correctamente, logrando una detección y mitigación de ciberataques en tiempo real. Una adecuada configuración garantiza el correcto funcionamiento del sistema sin afectar la comunicación dentro de la subestación.

No tener cuidado con los parámetros de personalización del IPS como perfiles, protocolos o direccionamientos puntuales necesarios, puede implicar un inconveniente mayor a la hora de implementar un IPS en una subestación, por ello, es ideal que quienes estén a cargo del manejo de este tipo de soluciones sean profesionales multidisciplinarios con conocimientos tanto en OT como IT o en su defecto que exista una convergencia a nivel práctico de estas dos áreas.

Existen aún numerosas oportunidades de investigación en este campo, particularmente en lo que respecta a optimización y aplicación de alternativas de protección para redes OT.

La efectividad de implementar un equipo de ciberseguridad en una red OT depende de varios factores como las capacidades técnicas del equipo IPS como el conocimiento de los operadores y administradores de la red OT que se desea proteger, esta combinación garantiza una protección efectiva frente a los ataques de personas malintencionadas.

6 REFERENCIAS

[1] J. Moteff, C. Copeland, y J. Fischer, «Critical Infrastructures: What Makes an Infrastructure Critical?».

[2] P. K. Garimella, «IT-OT Integration Challenges in Utilities», en 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu: IEEE, oct. 2018, pp. 199-204. doi: 10.1109/CCCS.2018.8586807.

[3] R. Flosbach, J. J. Chromik, y A. Remke, «Architecture and Prototype Implementation for Process-Aware Intrusion Detection in Electrical Grids», en 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France: IEEE, oct. 2019, pp. 42-4209. doi: 10.1109/SRDS47363.2019.00015.

[4] C. Konstantinou y M. Maniatakos, «Impact of firmware modification attacks on power systems field devices», en 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA: IEEE, nov. 2015, pp. 283-288. doi: 10.1109/SmartGridComm.2015.7436314.

[5] S. Major y E. Fekovic, «Securing intelligent substations: Real-time situational awareness», en 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia: IEEE, may 2014, pp. 711-715. doi: 10.1109/ENERGYCON.2014.6850504.

[6] K. A. Scarfone y P. M. Mell, «Guide to Intrusion Detection and Prevention Systems (IDPS)», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-94, 2007. doi: 10.6028/NIST.SP.800-94.

[7] A. L. Giri y S. Annamalai, «Intrusion Detection System for Local Networks – A Review Study», en 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India: IEEE, abr. 2022, pp. 1388-1393. doi: 10.1109/ICACITE53722.2022.9823433.

[8] Adrián Soucase Iranzo. «Implementacion de un Sistema de Prevencion de Intrusiones IPS en un modelo de red industrial.» (2021). *Escuela Técnica Superior de Ingeniería de Telecomunicación*, *Universitat Politècnica de València*. https://riunet.upv.es/handle/10251/178959

[9] P. Rathod y T. Hamalainen, «A Novel Model for Cybersecurity Economics and Analysis», en 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland: IEEE, ago. 2017, pp. 274-279. doi: 10.1109/CIT.2017.65.

[10] Sophos Whitepaper. «*The State of Ransomware in Critical Infrastructure*» *2024*. https://assets.sophos.com/X24WTUEQ/at/75tnw38cqsnrrv56wpwc78k/sophos-state-of-ransomware-critical-infrastructure-2024.pdf