UNIVERSIDAD TÉCNICA DE MANABÍ
Fundada en 1952

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Evaluación de la seguridad de las redes internas del área de los sistemas SCADA CNEL EP, unidad de negocios Manabí mediante OSSTMM y OPNET

Evaluation of the security of the internal networks of the SCADA CNEL EP Area, Manabí business unit through OSSTMM and OPNET

Autores

Luis Alonso Tapia Rivas

Viviana Demera Centeno

Facultad de Ciencias Informáticas, Universidad Técnica de Manabí, Portoviejo, Ecuador.

*Autor para correspondencia

Como citar el artículo:
Tapia Rivas, L. & Demera Centeno, V. (2023). Evaluación de la Seguridad de las Redes Internas del Área de SCADA CNEL EP, Unidad de Negocios Manabí. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, 7*(1), pp. 24–33. https://doi.org/10.33936/isrtic.v7i1.5558

Enviado: 16/02/2023;
Aceptado: 24/05/2023;
Publicado: 31/05/2023

Resumen

La transformación tecnológica que ha experimentado la sociedad ha generado un incremento de los ciberataques a nivel mundial, poniendo en riesgo a todos los sectores sociales y productivos de la sociedad que hacen uso de las tecnologías de la información, entre ellos el sector eléctrico, donde se utilizan con frecuencia sistemas de Control Supervisorio y Adquisición de Datos (SCADA). En Ecuador, el sector eléctrico es considerado un sector estratégico para el desarrollo del país y es administrado por la Corporación Nacional de Electricidad (CNEL EP). En este trabajo se evalúa la seguridad en el área SCADA de CNEL EP en la Unidad de Negocio Manabí aplicando el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) y utilizando el simulador OPNET. Se seleccionaron las subestaciones más importantes pertenecientes al área SCADA y se realizó una auditoría de acuerdo a la metodología para determinar el estado actual de la seguridad e identificar posibles vulnerabilidades. A su vez, con las vulnerabilidades identificadas, se diseñaron dos escenarios simulados de forma simplificada utilizando la herramienta OPNET para establecer el impacto de la explotación de una de estas vulnerabilidades en el funcionamiento de los servicios del área SCADA. Tras la obtención de los resultados, se concluyó que el nivel de seguridad del área SCADA es alto, aunque se identificó la existencia de interacciones no controladas en las operaciones que es necesario abordar, dado que, según los resultados obtenidos, la explotación de estas interacciones podría afectar significativamente al funcionamiento del área SCADA.

Palabras clave: SCADA; Redes; CNEL; OSSTMM; OPNET.

Abstract

The technological transformation that society has undergone has generated an increase in global cyber attacks, putting at risk all social and productive sectors of society that make use of information technologies, including the electric sector, where Supervisory Control and Data Acquisition (SCADA) systems are often used. In Ecuador, the electric sector is considered a strategic sector for the country's development and is managed by the Corporación Nacional de Electricidad (CNEL EP). This paper evaluates the security in the SCADA area of CNEL EP in the Manabí Business Unit by applying the Open Source Security Testing Methodology Manual (OSSTMM) and using the OPNET simulator. The most important substations belonging to the SCADA area were selected, and an audit was carried out according to the methodology to determine the current state of security and identify possible vulnerabilities. In turn, with the identified vulnerabilities, two simulated scenarios were designed in a simplified manner using the OPNET tool to establish the impact of exploiting one of these vulnerabilities on the operation of the SCADA area services. After obtaining the results, it was concluded that the level of security in the SCADA area is high, although the existence of uncontrolled interactions in operations was identified and needs to be addressed, given that according to the results obtained, the exploitation of these interactions could significantly affect the functioning of the SCADA area.

Keywords: SCADA; Networks; CNEL; OSSTMM; OPNET.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

1. Introducción

La Corporación Nacional de Electricidad (CNEL EP) es una empresa pública que fue crea el 13 de marzo de 2013 cuyo objetivo es prestar servicios públicos de distribución y comercialización de energía eléctrica en el Ecuador (CNEL EP, 2022). A su vez, la CNEL EP tiene varias unidades de negocios a través de todo el territorio nacional, siendo la Unidad de Negocios Manabí la encargada de la distribución y comercialización de energía eléctrica dentro de la provincia (CNEL EP, 2022).

Además, esta empresa tiene una fuerte relevancia para el Estado ecuatoriano dado que administra el sector eléctrico; un sector considerado estratégico de acuerdo con la Constitución de la República del Ecuador (CRE) lo que implica que "su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental" para el país (Asamblea Nacional Constituyente, 2008),

Esta particularidad le da a la infraestructura que administra la CNEL EP la connotación de infraestructura crítica, por cual es de vital importancia determinar posibles amenazas que pueden afectar su normal funcionamiento. Por otro lado, hay que considerar también los procesos de transformación tecnológica presente hoy por hoy en la sociedad y todos los nuevos retos en ciberseguridad que esto conlleva (Andrade y Yoo, 2019); en donde el sector eléctrico no queda excluido, dado el uso de sistemas informáticos para el control y monitoreo de la infraestructura como los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA), que no es más que un conjunto de programas, los cuales dan acceso a datos remotos de un proceso mediante la utilización de herramientas adecuadas (Rodríguez Penin, 2007); que en el caso de CNEL EP son los datos de la red de infraestructura eléctrica nacional.

A esto se le suma, la realidad existente en temas de ciberseguridad en América Latina y el Caribe, en donde en el 2020 existió un incremento del 57% de incidentes de ciberseguridad con respecto al año 2017 y 2018, y el triple de incidentes con respecto al año 2019 y en dónde el Ecuador consta entre los países con mayor cantidad de ciberataques (Díaz, 2021).

Esta realidad acarrea algún grado desconfianza por parte de la ciudadanía y, además pérdidas económicas en las Instituciones dado a la ausencia de mecanismos de control para la protección de la información y de los sistemas informáticos (Pazmiño Vallejo, 2015). De ahí que en la sociedad digitalizada en la que se vive, son necesarios mecanismos que salvaguarden la información que manejan las empresas, los gobiernos y las personas evitando de esta manera ser blancos fáciles de espionaje, delitos u otros tipos de ataques que vulneren la integridad institucional y personal (Gamboa Suárez, 2020).

Por esto, la importancia de la seguridad informática radica en establecer estrategias y métodos para la protección de los sistemas y del entorno en que funcionan (Ferreira Alves, 2018); así como la organización de políticas para la preservación y el uso correcto de los datos, procurando resguardar la confidencialidad, integridad y disponibilidad de estos (García Pierrat y Vidal Ledo, 2016).

Adicionalmente, hay que mencionar que la seguridad informática tiene varios enfoques; entre estas la seguridad de red, que puede entenderse como aquellas medidas que buscan proteger a una red informática de intrusos; ya sean estos atacantes dirigidos o malwares oportunistas (Gamboa Suárez, 2020).

La ausencia o falencias de estas estrategias y mecanismo de seguridad informática conllevan a graves consecuencias; más aún en el sector eléctrico ya que de este depende el resto de los servicios vitales de un país, tal y como lo sostiene Calzada Hinojosa (2021). Algo similar menciona Carreño Pérez (2019), el cual sostiene que el sistema eléctrico es una parte indispensable de un país y por tanto debe ser una prioridad ya que de este depende toda la infraestructura nacional.

De ahí que dado el uso de sistemas informáticos en infraestructura crítica es necesario contar con sistemas actualizados periódicamente y tener en consideración aquellas vulnerabilidades y amenazas que puede afectar a la organización (Rosas et al., 2020); así como realizar revisiones periódicas de las vulnerabilidades para tener un registro (González Tandazo, 2016).

En este sentido, en la literatura existen diversas metodologías para la evaluación de la seguridad además de diferentes trabajos que realizan comparativas entre éstas; como el trabajo realiza por Gordón Revelo (2017), en dónde compara las metodologías: Solicitud del Proyecto de Seguridad Open Web (OWASP), National Institute of Standards and Technology Special Publication 800-115 (NIST SP 800-115), la cual es la Guía técnica de pruebas y evaluación de la seguridad de la información; y Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM).

En esta comparativa, Gordón Revelo (2017) concluye que la OSSTMM tiene un enfoque de análisis más completo de la seguridad actuando en los ámbitos humano, físico, de medios inalámbricos, telecomunicaciones y de redes de datos. Además, sostiene que la metodología OSSTMM tiene un valor agregado al poseer una métrica cuantitativa que permite cuantificar de manera global el estado actual de la seguridad operacional como lo es los Valores de Evaluación de Riesgos (RAV). Lo mencionado por Gordón Revelo (2017) es compartido por Medina Becerra et al. (2019), los cuales añaden que esta metodología cubre todos los escenarios dónde se pueden presentar vulnerabilidades y además sugiere el uso de la metodología OSSTMM para la evaluación de la seguridad en los sistemas SCADA.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Con respecto a la metodología OSSTMM es un estándar de seguridad profesional que proporciona un marco detallado que permite realizar evaluaciones de seguridad a sistemas, la cual fue creada en el 2001 por Pet Herzog en conjunto con más de 150 colaboradores (ISECOM, 2010). Esta metodología considera si existe o no una separación de algún tipo entre la amenaza y el activo, pudiendo ser ésta una barrera física o lógica, la transformación de la amenaza en algo inofensivo o la destrucción de la amenaza (ISECOM, 2010).

De esta manera la metodología OSSTMM, considera los controles de dos tipos. Por un lado, están los controles de clase A, en lo que se incluyen todos aquellos controles interactivos; mientras que en los controles de clase B, están aquellos controles que se relacionan con la defensa de los procesos (ISECOM, 2010). El estado de seguridad que tiene las operaciones queda determinado por el RAV, el cual indica cuan grande es la superficie de un posible ataque, siendo un valor de 100 un perfecto equilibrio entre las operaciones, las limitaciones y los controles (ISECOM, 2010).

Además, es necesario mencionar que la aplicación de la metodología OSSTMM consiste en la realización de una auditoría que involucra en primer lugar la recopilación de información y datos; como la recopilación de información sobre sistemas, redes y aplicaciones, la revisión de políticas y procedimientos de seguridad y la identificación de los activos críticos que necesitan protección (ISECOM, 2010).

En segundo lugar, se debe realizar un análisis de amenazas en donde se identifican las amenazas potenciales sobre estos activos y la determinación de la probabilidad de que se produzcan; para posteriormente realizar una evaluación de vulnerabilidades en donde identifican las vulnerabilidades del sistema que pueden ser explotadas por un atacante; lo que incluye pruebas de penetración y evaluaciones de vulnerabilidades de sistemas, redes y aplicaciones (ISECOM, 2010).

Después, se realiza un análisis del impacto que tendría un ataque exitoso a unos de los activos expuestos; por lo que se realiza la evaluación de los activos críticos, los procesos empresariales y los datos que podrían verse afectados. Enseguida se realiza un análisis de protección el cual se enfoca en evaluar la efectividad de los controles de seguridad implementados; e incluye la revisión de políticas y procedimientos de seguridad, la evaluación de la implementación de los controles de seguridad y la determinación de la efectividad de los controles (ISECOM, 2010).

Finalmente, la auditoría involucra un análisis de verificación en donde se incluye la evaluación de los registros y registros de auditoría para determinar si se han producido violaciones de seguridad y la identificación de oportunidades de mejora en los controles de seguridad (ISECOM, 2010).

Además de estas metodologías, para las evaluaciones de seguridad también se suelen utilizar sistemas de simulación sobre todo para la detección de anomalías dentro del funcionamiento de una red (García Alfaro et al., 2014). De ahí que existan trabajo como el de Rahman et al. (2009), los cuales realizan una revisión de distintas herramientas de simulación y modelados de redes (ver Tabla 2), entre éstas OPNET; de la cual concluye que ofrece una gran cantidad de variantes acerca de redes objetivos.

Del mismo modo, Njova (2021) menciona que en su trabajo sobre la evaluación del protocolo Distributed Network Protocol version 3 (DNP3) sobre subestaciones de unidades operativas del este de Sudáfrica en serie para la mejora del rendimiento de los sistemas SCADA, OPNET fue una herramienta valiosa para la simulación de dispositivos de red y monitoreo de su rendimiento sin necesidad construir una red real con los costos que esto involucraría.

comparativos sobre el impacto de las posibles vulnerabilidades detectadas en las redes mediante el uso de herramientas de simulación, para finalmente validar los resultados alcanzados sobre el estado de la seguridad de las redes internas del área de los sistemas SCADA.

2. Materiales y Métodos

Este trabajo se concibió como experimental (Hernández Sampieri et al., 2014) dada la manipulación de las variables mediante la aplicación de una metodología de evaluación del riesgo de la seguridad en las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocio Manabí, y modelado de escenarios en herramientas de simulación para determinar el impacto de una posible explotación de vulnerabilidades en la infraestructura eléctrica.

Por otro lado, la connotación del estudio requirió que una investigación de tipo mixta (Hernández Sampieri et al., 2014), dado que se combina tanto métodos cuantitativos como cualitativos; así como de naturaleza exploratoria, ya que permite examinar e investigar a fondo un problema con el objetivo de hacer un diagnóstico (Hernández Sampieri et al., 2014) ; descriptiva, ya que los datos obtenidos de fuentes oficiales o documentales permiten identificar la realidad del problema en análisis (Albareda Herrera, 2011); correlacional, ya que se miden las relaciones entre las variables en estudio (Curbelo Martínez et al., 2016) ; explicativa, ya que se busca encontrar las razones por las cuales la seguridad de las redes pueden estar siendo afectadas (Mejía Jervis, 2020), y documental, ya que se lleva a cabo una revisión de libros, artículos y otros documentos relacionados con el estudio (Gonzáles, 2020).

En cuanto a la metodología de evaluación de la seguridad a aplicar, esta fue seleccionada a partir de la comparación realizada entre las metodologías OSSTMM, NIST 800-115 y OWASP por Gordón Revelo (2017), tomando como criterios el Factor digital, Factor físico, Factor social, las Métricas, los Informes y la Guía técnica (ver Tabla 2).

A partir del trabajo por Gordón Revelo (2017), se puede evidenciar que de las metodologías comparadas, la OSSTMM tiene un enfoque más integral y completo sobre la seguridad; lo cual es compartido por autores como Medina Becerra et al.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

Tabla 1: Comparativa de herramientas de simulación y modelados de redes.
Fuente: García Alfaro et al. (2014), Rahman et al. (2009) y Njova (2021)

Características	Simuladores					
	OPNET/Riverbed Modeler	**NS-2**	**NetSim**	**MaRs**	**NS-3**	**Omnet++**
Tipo de simulación	Discreta y continua	Discreta	Discreta	Discreta y continua	Discreta	Discreta y continua
Interfaz gráfica de usuario (GUI)	Sí	No	Sí	Sí	No	Sí
Soporte de protocolos de red	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, OSPF, BGP, MPLS, RSVP, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Soporte limitado, incluyendo TCP, UDP, IPv4, etc.	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, etc.	Amplio soporte, incluyendo TCP, UDP, IPv4, IPv6, etc.
Modelado de dispositivos de red	Amplio soporte.	Soporte limitado	Amplio soporte.	Soporte limitado.	Amplio soporte.	Amplio soporte
Modelado de tráfico	Amplio soporte.	Soporte limitado.	Soporte limitado.	Soporte limitado.	Amplio soporte.	Amplio soporte.
Escalabilidad	Alta	Media	Alta	Media	Alta	Alta
Licencia	Requiere Licencia/Tiene versión de prueba	Gratuita	Requiere Licencia	Gratuita	Gratuita	Gratuita

(2019), quienes además recomiendan esta metodología para la evaluación de los sistemas SCADA. En virtud de estas características se aplicó la metodología OSSTMM para la evaluación de la seguridad en las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí.

Del mismo modo, como herramienta de simulación se seleccionó OPNET, a partir de los criterios de autores como Rahman et al. (2009), Ashraf et al. (2021) o Njova (2021); quienes exponen el amplio abanico de redes que la herramienta puede simular, así como las ventajas que ofrece OPNET al simular redes complejas. Adicionalmente se hizo uso de técnicas e instrumentos como entrevistas y fichas de observación a la máxima autoridad y al jefe del departamento de informática de la Unidad de Negocios.

En lo que respecta a la población de estudio esta corresponde a las redes internas del área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, la misma que está integrada por un total de 30 subestaciones distribuidas en ubicaciones estratégicas a través de toda la provincia teniendo una capacidad de 505/625 Megavoltamperio (MVA) de potencia.

De todas ellas, se seleccionaron un total de 13 subestaciones; de acuerdo con la información proporcionada por la Unidad de Negocios de Manabí sobre aquellas subestaciones que soportan mayor carga operativa. De ahí que las subestaciones seleccionadas distribuyen cerca del 65% de la energía de la provincia de Manabí, encontrándose ubicadas dentro de los cantones Portoviejo, Manta, Rocafuerte, Montecristi y Jaramijó.

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Tabla 2: Análisis comparativos de las metodologías de seguridad informática.
Fuente: Obtenido de (Gordón Revelo, 2017).

FACTORES	Metodologías		
	OSSTMM	NIST 800-115	OWASP
Factor Digital	X	X	X
Factor Físico	X		
Factor Social	X	X	
Métricas	X		
Informes	X	X	
Guía Técnica			X

Para el procesamiento de datos se utilizó se usó la plataforma de Google Colab junto con el lenguaje de programación Python en su versión 3.9.16, así como sus librerías NumPy, Pandas y SciPy, en sus versiones 1.22.4, 1.4.4, 1.10.1 respectivamente para aplicar métodos estadísticos para la validación de los resultados obtenidos.

Es así como el presente trabajo se realizó en cuatro fases; enfocándose la primera de ellas en la búsqueda y revisión del estado del arte sobre la a evaluación de la seguridad en los sistemas SCADA, en especial en su aplicación en el sector eléctrico; además del análisis de los estándares de seguridad informática y la selección de la metodología y el simulador para evaluar la seguridad de las redes internas el área de los sistemas SCADA.

Por otro lado, en la segunda fase se aplicó la metodología seleccionada en 13 subestaciones eléctricas con el objetivo de evaluar la seguridad; realizando también visitas in situ en cada una de las subestaciones identificando de esta manera activos de valor y aquellos mecanismos establecidos para la defensa de éstos ante posibles amenazas, tales como áreas restringidas y mecanismos de acceso y autenticación a esas áreas. Por otra parte se realizó la revisión de documentación sobre los sistemas, las políticas de seguridad implementadas, auditorías realizadas, y demás documentación que permitió conocer los procesos que se desempeñan en las instalaciones; así como el escaneo de la redes y equipos informáticos mediante herramientas de auditoría informática para identificar posibles vulnerabilidades.

Finalmente, los resultados obtenidos sobre el estado de la seguridad se registraron y tabularon en una matriz de Excel (ver Figura 1), que muestra de manera cuantitativa el estado de seguridad y la cantidad de vulnerabilidades encontradas en las redes internas del área de los sistemas SCADA.

Del mismo modo, en la tercera fase de la investigación, se identificó la vulnerabilidad más crítica identificada en los sistemas SCADA, basándose en los resultados obtenidos en la segunda fase, y se construyeron de forma simplificada dos escenarios simulados en dónde se representaron los servicios de red más utilizados en el área de los sistemas SCADA para evaluar la repercusión que podría tener si se explotara esta

Figura 1: Matriz Excel para determinar el estado de la seguridad proporcionada por la Metodología OSSTMM

vulnerabilidad. El primer escenario imitó las condiciones actuales con la vulnerabilidad presente y el segundo escenario mostró el funcionamiento de la red al explotar la vulnerabilidad. Para esto en OPNET se simuló el tiempo de respuesta de solicitudes Web (protocolo HTTP) desde las subestaciones hacia al servidor central del área de los sistemas SCADA mediante una conexión a internet, dado que los servicios webs mediante el protocolo HTTP es el más usado para compartir datos entre los sistemas SCADA del área. Adicionalmente, se añadió en el segundo escenario un equipo para simular un atacante que envía peticiones Ping con un paquete de 65527 bytes, en intervalos de un segundo de manera constante hacia el servidor (ver Figura 2), esto como una manera efectiva de simular un ataque DoS intenso, saturar el ancho de banda de la red y sobrecargar los recursos del sistema objetivo dentro de un entorno de simulación simplificado; dado que un solo paquete de este tamaño, equivaldría a que 1024 computadora realicen solicitudes ping hacia el servidor con un tamaño de paquete predeterminado (aproximadamente 64 bytes). De esta manera, los tiempos de respuesta del servicio simulado fueron medidos mediante los mecanismos ofrecidos por la herramienta de simulación seleccionada para luego ser analizados.

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5588**

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

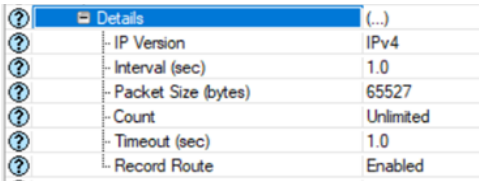

Figura 2: Detalle de la configuración de las solicitudes Ping en la herramienta OPNET.

Finalmente, en la última etapa se evaluaron los resultados obtenidos en las simulaciones, lo que permitió determinar la validez de la hipótesis planteada; utilizando la prueba de normalidad de Shapiro-Wilk y la prueba de Wilcoxon lo que permitió la comparación de las dos muestras experimentales relacionadas (Wilcoxon, 1945) y de esta manera llegar a las conclusiones.

3. Resultados y Discusión

Luego de la aplicación de la metodología de evaluación OSSTMM en las 13 subestaciones eléctricas objeto del estudio se lograron identificar como activos críticos los servidores de control SCADA, bases de datos de información de infraestructura eléctrica, nodos de red de alta prioridad, sensores y equipos de control en subestaciones eléctricas. Por otro lado, al revisar las políticas y procedimientos de seguridad, se encontró que se necesitaban mejoras significativas en la gestión de contraseñas, la autenticación de usuarios y la monitorización de eventos en tiempo real.

Del mismo modo, se identificaron como amenazas los ataques de denegación de servicio (DoS) debido a la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa, malware, ingeniería social y la explotación de vulnerabilidades en sistemas SCADA; llegando a determinar que existe un alto riesgos de explotación debido a la falta de controles de seguridad efectivos en algunas de las subestaciones evaluadas. Así también al realizar pruebas de penetración en las aplicaciones, se identificaron vulnerabilidades de inyección de Lenguaje de Consulta Estructurada (SQL) y falta de cifrado en la transmisión de datos en algunas aplicaciones utilizadas al interior de las instalaciones.

Por otra parte, mediante el análisis del impacto de un ataque exitoso a los activos críticos identificados anteriormente, se determinó que el impacto sería significativo en términos de interrupción del suministro eléctrico y posible daño a la infraestructura; además se encontró, mediante una evaluación de la implementación de los controles de seguridad, que no se habían efectuado controles adecuados para mitigar las vulnerabilidades identificadas.

Así mimo, se evaluó la efectividad de los controles de seguridad y se determinó que los controles existentes eran insuficientes para mitigar los riesgos identificados. También, mediante la evaluación de los registros y registros de auditoría, en donde se evaluaron los registros de auditorías, se encontraron varias anomalías de seguridad, incluyendo accesos no autorizados y eventos sospechosos en los registros de actividad del sistema.

De ahí que al calcular la métrica RAV, se obtuvo en las subestaciones del catón Portoviejo un valor RAV promedio de 91.3905 puntos. En este cantón se evaluó a un total de cinco subestaciones (ver Tabla 3); en donde la subestación PORTOVIEJO 1 obtuvo un RAV de 91.3563 puntos, la subestación PORTOVIEJO 2 un RAV DE 93.7277 puntos, la subestación PORTOVIEJO 3 obtuvo un RAV de 90.6195, la subestación PORTOVIEJO 4 un valor RAV de 92.0465 y la subestación CRUCITA un valor RAV de 89.8636 puntos.

Tabla 3: Resultados auditoria OSSTMM Portoviejo.

Fuente: Investigador.

PORTOVIEJO	
SUBESTACIÓN	**RAV**
PORTOVIEJO 1	91,3563
PORTOVIEJO 2	93,7227
PORTOVIEJO 3	90,6195
PORTOVIEJO 4	92,0465
CRUCITA	89,8636

Con respecto al cantón Montecristi, se evaluaron un total de dos subestaciones (ver Tabla 5). En el caso de la subestación MONTECRISTI 1 el valor RAV obtenido es de 92.6508 puntos, mientras que en la subestación MONTECRISTI 2 se obtuvo 90.5323 puntos RAV. En el caso del cantón Montecristi el valor RAV promedio obtenido por las subestaciones es de 91.5915 puntos.

Tabla 4: Resultados auditoria OSSTMM Manta.

Fuente: Investigador.

MANTA	
SUBESTACIÓN	**RAV**
MANTA 1	94,6910
MANTA 2	92,9107
MANTA 3	91,3060
MANTA 4	89,4675

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

Con respecto al cantón Montecristi, se evaluaron un total de dos subestaciones (ver Tabla 5). En el caso de la subestación MONTECRISTI 1 el valor RAV obtenido es de 92.6508 puntos, mientras que en la subestación MONTECRISTI 2 se obtuvo 90.5323 puntos RAV. En el caso del cantón Montecristi el valor RAV promedio obtenido por las subestaciones es de 91.5915 puntos.

Tabla 5: Resultados auditoria OSSTMM Montecristi.

Fuente: Investigador.

MONTECRISTI	
SUBESTACIÓN	**RAV**
MONTECRISTI 1	92,6508
MONTECRISTI 2	90,5323

En el caso del cantón Rocafuerte, se evaluó la subestación ROCAFUERTE obteniendo un valor RAV de 92,4415 puntos (ver Tabla 6). De igual manera, se evaluó la subestación JARAMIJÓ ubicado en el cantón del mismo nombre en donde se obtuvo como resultado un valor de 90.7615 puntos RAV (ver Tabla 7).

Tabla 6: Resultados auditoria OSSTMM Rocafuerte.

Fuente: Investigador

ROCAFUERTE	
SUBESTACIÓN	**RAV**
ROCAFUERTE	92,4415

Tabla 7: Resultados auditoria OSSTMM Jaramijó.

Fuente: Investigador.

JARAMIJÓ	
SUBESTACIÓN	**RAV**
JARAMIJÓ	90,7615

Si bien los valores RAV obtenidos en las subestaciones evaluadas son cercanos a 100; de hecho, el valor medio de RAV de las subestaciones evaluadas es del 91.5217 puntos, lo que puede ser considerada como una seguridad alta; estos resultados reflejan la existencia de interacciones no controladas en las operaciones mencionadas en los párrafos anteriores. De ahí que de todas estas limitaciones y vulnerabilidades detectadas, se consideró para realizar los escenarios simulados la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa; debido a que la vulnerabilidad puede ser explotada de forma remota, tiene un alto riesgo de afectación (Loukas y Öke, 2010) del área de los sistemas SCADA y, además, esta vulnerabilidad es constante en todas las subestaciones evaluadas.

A partir de esto se consideró la simulación de un Ataque de Denegación de Servicio (DoS, por sus siglas en inglés) en la herramienta OPNET aprovechando la vulnerabilidad detectada, bajo los parámetros expresados en la Tabla 8, y con base a lo mencionado por Loukas y Öke (2010) , quien además menciona que los ataques DoS “son fáciles de lanzar, mientras que defender un recurso de red contra ellos es desproporcionadamente difícil”.

Tabla 8: Parámetros de simulación utilizados en los escenarios.

Fuente: Investigador.

PARÁMETRO	VALOR
Protocolo de enrutamiento	RIP (Routing Information Protocol)
Protocolo de transporte	TCP (Transmission Control Protocol)
Carga de tráfico	HTTP, FTP, BD
Tamaño de paquete	1500 bytes
Latencia	10 ms
Ancho de banda	10 Mbps
Pérdida de paquetes	0%
Tiempo de simulación	5 horas

De esta manera se estableció dos escenarios de simulación; en donde el primer escenario (ver Figura 3), considerado el de referencia, mostró el funcionamiento actual de las subestaciones evaluadas al conectarse con el servidor central del área de los sistemas SCADA mediante la internet; mientras que en el segundo escenario (ver Figura 4) simuló la explotación de la vulnerabilidad mediante un ataque DoS desde un equipo remoto en la internet.

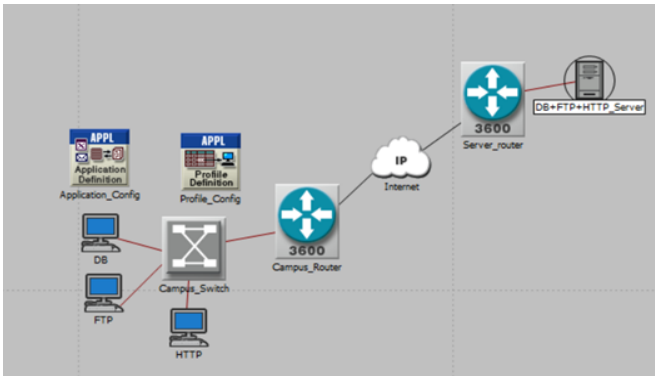

Figura 3: Experimento de simulación 1 (Escenario base).

En cada uno de estos escenarios existieron tres equipos informáticos (modelo ethernet_wkstn) que simularon servicios de base de datos (DB), transferencias de archivos (protocolo FTP) y servidor web (protocolo HTTP) con el objetivo de establecer condiciones de funcionamiento similares a la realidad relacionados con el congestionamiento de la red; además de un equipo adicional que funcionó como servidor (modelo ethernet_server). Estos equipos accedieron a la internet mediante dos router (modelo CS_3640_4s_e5_fe1_tr1_sl6), el cuales funcionaron como puerta de enlace.

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

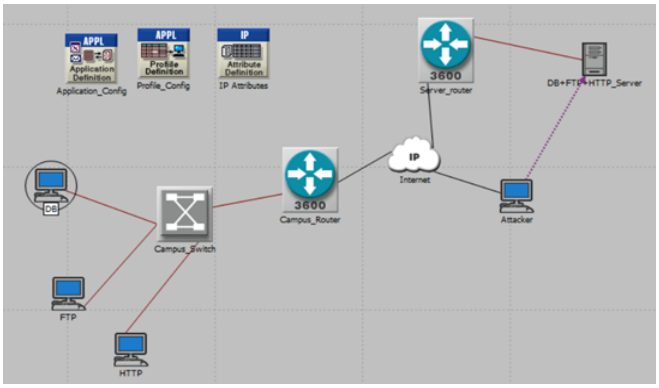

Figura 4: Experimento de simulación 2 (Escenario de explotación de la vulnerabilidad).

Cabe señalar también que para la simulación del ataque DoS, se añadió un equipo (modelo ethernet_wkstn) que funcionó de atacante enviando solicitudes Ping (ver Figura1) con un paquete de 65527 bytes mediante la Internet, en intervalos de un segundo de manera constante hacia el servidor y, que además para realizar la comparativa de los diferentes resultados se utilizó la métrica de Page Response Time (PRT), cuya unidad de medida es en segundos (s) y además viene incluida en el OPNET.

Figura 5: Valores PRT para el servicio HTTP durante la simulación del primer escenario.

De esta manera, en la simulación del primer escenario (ver Figura 3), se obtiene como resultado que el PRT (ver Figura 5) muestra un comportamiento estable; ya que durante las 5 horas que fue el tiempo de simulación, la métrica se mantuvo cercana al valor de 2.2 segundos; aunque cabe señalar que en un primer momento se obtuvo un valor inicial de 2 segundos y durante los primeros 20 minutos hubo un pico máximo en la métrica con un valor muy cercano a los 2.6 segundos de PRT.

Mientras que para el segundo escenario (ver Figura 4) se obtuvo como resultados (ver Figura 6) un valor inicial para el PRT de 4.5 segundos, lo que representa una demora de 2,5 segundos con respecto al valor inicial obtenido en el primer escenario. Del mismo modo en la Figura 6 se puede observar a medida que pasa el tiempo de la simulación, los resultados obtenidos en el valor del PRT disminuye hasta alcanzar un valor cercano a 3.5 segundos cerca de las dos horas de simulación. Este valor se mantiene estable hasta las cuatro horas y cuarenta minutos de simulación, tiempo después del cual no se observa ningún tipo de datos, lo que indica que el ataque DoS provocó una sobrecarga en el servidor que lo llevó a dejar de responder después de un cierto período de tiempo, lo que explicaría por qué no se recibieron datos durante todo el tiempo de simulación.

Esto resultados dan a entender que en una hipotética explotación de la vulnerabilidad de conexión a servicio remotos desde fuera de la red corporativa mediante un ataque DoS, la afectación sería significativa; tal y como también lo establecen los resultados de la auditoría OSSTMM, a tal punto que puede dejar fuera de operación los sistemas del área de los sistemas SCADA de CNEL EP, Unidad de Negocio Manabí.

Finalmente con los resultados de la simulación obtenidos se aplicaron dos pruebas estadísticas. Por un lado se aplicó la prueba de Shapiro-Wilk, la cual permitió conocer que los datos obtenidos no tenían una distribución normal; determinando de esta manera el uso de la prueba de Wilcoxon, una prueba estadística no paramétrica, para la validación de la hipótesis planteada en este estudio.

De ahí que la prueba de Wilcoxon determinó que existen evidencias suficientes para establecer que la aplicación de una metodología de evaluación del riesgo en seguridad informáticas y simuladores de red permitió conocer el estado de la seguridad y el impacto de las vulnerabilidades en las redes internas en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, dado que en la prueba mencionada se obtuvo un valor P de 0.0003, de modo que se rechazó la hipótesis nula; con un nivel de confianza del 95% y un nivel de significancia del 5%, al ser el valor de $P < 0.05$.

Figura 6: Valores PRT para el servicio HTTP durante la simulación del segundo escenario.

4. Conclusiones

En los últimos años ha habido un aumento significativo en los ciberataques, lo que ha generado desconfianza en los usuarios y ha provocado pérdidas económicas en instituciones públicas y privadas. En particular, Ecuador se encuentra entre los países con mayor cantidad de incidencias en temas de ciberseguridad,

e-ISNN 2550-6730 | Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023 | DOI: 10.33936/isrtic.v7i1.5588

lo que subraya la importancia de abordar esta problemática en el sector eléctrico. Dado el papel crucial del sector eléctrico en el desarrollo del país, es esencial contar con sistemas SCADA para el control y monitoreo de la infraestructura eléctrica. Sin embargo, es necesario implementar estrategias y métodos que protejan la confidencialidad, integridad y disponibilidad de los datos, así como políticas para la revisión periódica de la seguridad interna mediante la aplicación de metodologías de evaluación de la seguridad como la OSSTMM.

La metodología OSSTMM se enfoca en una evaluación integral de la seguridad de los sistemas y las comunicaciones, lo que permitió establecer que el área de los sistemas SCADA evaluada tiene una seguridad del 91.72% en su superficie de ataque potencial. También se identificaron algunas limitaciones comunes existentes en las subestaciones pertenecientes al área evaluada al aplicar la auditoría OSSTMM. La explotación de alguna vulnerabilidad dentro del área SCADA de CNEL EP, Unidad de Negocios Manabí, podría afectar de manera significativa el funcionamiento de la infraestructura eléctrica, llegando incluso a la interrupción total de los servicios, como en el caso de la posibilidad de acceso no autorizado al servidor de control SCADA desde fuera de la red corporativa. Además, se encontró que la aplicación de una metodología de evaluación del riesgo en seguridad informática y simuladores de red permitió conocer el estado de la seguridad y el impacto de las vulnerabilidades en las redes internas en el área SCADA de CNEL EP, Unidad de Negocios Manabí, con un nivel de significación del 5%.

Por otor lado, durante el desarrollo de este trabajo se encontraron limitaciones para acceder a información sobre el área de los sistemas SCADA de la Unidad de Negocios Manabí, ya que el sector eléctrico en Ecuador se considera como sector estratégico y, por lo tanto, parte de esta información es reservada o confidencial. Además, cabe destacar que el objetivo principal de este estudio fue evaluar la seguridad de las redes internas en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, para determinar su estado actual. Por tanto, el desarrollo de soluciones y medidas correctivas, como en el caso de un ataque DoS, va más allá del alcance de este estudio. Sería necesario llevar a cabo una investigación más detallada para identificar y evaluar soluciones adecuadas, dada la connotación estratégica que tiene el sector eléctrico en Ecuador. Es importante destacar que, aunque se utilizó una simulación de red en este trabajo, se reconoce que la configuración de red real en el área de los sistemas SCADA de CNEL EP, Unidad de Negocios Manabí, es significativamente más grande y compleja de lo que se puede simular con los recursos disponibles. Por lo tanto, se deben considerar diseñar estrategias de protección y medidas correctivas con precaución.

Además, el presente trabajo permite explorar diversas líneas de investigación futura. En primer lugar, es recomendable realizar un análisis más detallado de las vulnerabilidades específicas de la infraestructura eléctrica y aplicar técnicas de protección adecuadas para garantizar la seguridad de los sistemas SCADA. Además, es importante investigar más a fondo los ataques cibernéticos recientes en el sector eléctrico, su impacto y las medidas de protección implementadas para evitar futuros incidentes.

Por otro lado, sería útil evaluar las metodologías de evaluación de seguridad actuales utilizadas en el sector eléctrico y proponer nuevas metodologías más efectivas y eficientes. Esto podría incluir la comparación de las metodologías actuales con los marcos de seguridad internacionales y la recomendación de mejores prácticas.

Asimismo, sería beneficioso desarrollar técnicas de detección de ataques cibernéticos en tiempo real en el sector eléctrico y su aplicación en los sistemas SCADA. Esto podría incluir la implementación de sistemas de monitoreo y alerta temprana para detectar posibles amenazas a la infraestructura eléctrica y permitir una respuesta rápida y efectiva.

Finalmente, se debe investigar sobre los desafíos de seguridad y privacidad que surgen con la adopción de tecnologías emergentes en el sector eléctrico, como la Internet de las cosas (IoT) y el procesamiento en la nube, y las medidas que deben tomarse para proteger la infraestructura eléctrica. En este sentido, es necesario evaluar los riesgos asociados con la adopción de estas tecnologías y proponer medidas de protección adecuadas.

Contribución de los autores

Luis Alfonso Tapia Rivas: Conceptualización, Metodología, Software, Análisis formal, Redacción – borrador original del artículo, Visualización, Investigación. **Viviana Demera Centeno**: Supervisión, Redacción – revisión y edición del artículo.

Conflictos de interés

Los autores declaran no tener ningún conflicto de interés.

Referencias bibliográficas

Albareda Herrera, J. M. (2011). *Consideraciones sobre la investigación científica.* Vita Brevis.

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48,* 102352. https://doi.org/10.1016/j.jisa.2019.06.008

Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. *Registro Oficial,* 449(20), 25–2021. www.lexis.com.ec

Ashraf, S., Shawon, M. H., Khalid, H. M., & Muyeen, S. M. (2021). Denial-of-Service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways. *Sensors, 21*(19). https://doi.org/10.3390/s21196415

Calzada Hinojosa, S. J. (2021). Ciberseguridad en la protección

INFORMÁTICA Y SISTEMAS
Revista de Tecnologías de la Informática y las Comunicaciones

Facultad de Ciencias Informáticas
Universidad Técnica de Manabí
Av. Urbina y Che Guevara, Portoviejo, Ecuador
revista.iys@utm.edu.ec

de infraestructuras críticas eléctricas. R*evista Telemática, 20(1),* 36–46.

Carreño Pérez, J. C. (2019). *Metodología para evaluación de ciber vulnerabilidad en sistemas de transmisión de energía eléctrica "EVULCIB", estudio de caso subestación eléctrica de 230kV ubicada en la ciudad de Bogotá-Colombia.* [Tesis de Maestría]. Universidad Distrital Francisco José de Caldas.

CNEL EP. (2022). *Historia.* Disponible en https://www.cnelep.gob.ec/historia/Curbelo Martínez, G., Cortés Cortés, M., y Pérez Fernández, A. del C. (2016). Metodología para el análisis de correlación y concordancia en equipos de mediciones similares. *Revista Universidad y Sociedad, 8*(4), 65-70.

Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe. *Desarrollo productivo (228)*

Ferreira Alves, M. (2018). Ciberseguridad en la infraestructura crítica mediante el sistema SCADA en planta de tratamiento de agua de Lima. *Revista Escuela de Guerra del Ejército del Perú, 02*(03), 48–55.

Gamboa Suárez, J. L. (2020). I*mportancia de la seguridad informática y ciberseguridad en el mundo actual.* Tesis de posgrado. [Tesis de Maestría]. Universidad Piloto de Colombia.

García Pierrat, G., y Vidal Ledo, M. J. (2016). Informatics and security: an important topic for managers. *Infodir Revista de Información para la Dirección en Salud, 12*(22), 47-58.

García-Alfaro, J., Romero-Tris, C., y Rubio-Hernan, J. (2014). *Simulaciones Software para el Estudio de Amenazas contra Sistemas SCADA.* Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. pp. 151-156

Gonzáles, G. (2020). *Investigación documental: características, estructura, etapas, tipos, ejemplos.* Disponible en https://www.lifeder.com/investigacion-documental/

González Cruz, R. (2018). R*ediseño del software Amplifiers para el diseño de amplificadores de pequeña señal con BJT y FET.* Universidad Central" Marta Abreu" de Las Villas, Facultad de Ingeniería.

González Tandazo, N. (2016). *Evaluar las vulnerabilidades de seguridad existentes en la red del sistema SCADA de la EERSSA.* [Tesis de Maestría]. Universidad de Cuenca.

Gordón Revelo, D. S. (2017). *Análisis de estrategias de gestión de seguridad informática con base en la metodología open source security testing methodology manual (osstmm) para la intranet de una institución de educación superior.* [Tesis de Maestría]. Universidad Espíritu Santo.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodología de la investigación.*

ISECOM. (2010). OSSTMM.3. Disponible en https://www.isecom.org/OSSTMM.3.pdf

Loukas, G., y Öke, G. (2010). Protection against denial of service attacks: A survey. *Computer Journal, 53*(7), 1020–1037. DOI: https://doi.org/10.1093/COMJNL/BXP078

Medina Becerra, F. A., Tirano Vargas, J. A., y Vargas Barrera, D. A. (2019). Metodología para la Ejecución de Evaluación de Ciber-Vulnerabilidades en los Sistemas ICS-SCADA de los Agentes del Sistema Interconectado Nacional. *Revista Infometric@-Serie Ingeniería, 1*(1).

Mejía Jervis, T. (2020). *Investigación explicativa: características, técnicas, ejemplos.* Disponible en https://www.lifeder.com/investigacion-explicativa/

Njova, D. (2021). *Evaluating of DNP3 protocol over serial eastern operating unit substations and improving SCADA performance.* University of South Africa.

Pazmiño Vallejo, L. M. (2015). *Calidad de la gestión en la seguridad de la información basada en la norma ISO/IEC 27001, en instituciones públicas, en la ciudad de Quito D.M.* [Tesis de Maestría]. Pontifica Universidad Católica del Ecuador.

Rahman, M. A., Pakštas, A., y Wang, F. Z. (2009). Network modelling and simulation tools. *Simulation Modelling Practice and Theory, 17*(6), 1011–1031. DOI: https://doi.org/10.1016/J.SIMPAT.2009.02.005

Rodríguez Penin, A. (2007). *Sistemas SCADA: guía práctica - Aquilino Rodríguez Penin - Google Libros.* Disponible en https://books.google.com.ec/books?id=Sai-a0WQw24Cyprintsec=frontcoverysource=gbs_ge_summary_rycad=0#v=onepageyqyf=false

Rosas, W. A., Medina, F. A., & Mesa, J. A. (2020). Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas. Revista Espacios, 41(07).

Ruiz, M., y Ulloa, C. (2013). *Diseño y Evaluación de Redes usando OPNET.* Universidad Técnica Federico Santa María.

Wilcoxon, F. (1945). Some Uses of Statistics in Plant Pathology. *Biometrics Bulletin,* 1(4), 41. DOI: https://doi.org/10.2307/3002011

e-ISNN 2550-6730 | **Vol. 7, Núm. 1 (24-33): Enero-Junio, 2023** | **DOI: 10.33936/isrtic.v7i1.5588**