INGENIERÍAS USBMed

https://revistas.usb.edu.co/index.php/ingUSBmed

ARTÍCULO DE REFLEXIÓN

Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA

Methodological Proposal for the Cybersecurity Audit Applied to a SCADA System

Ricardo Alonso Torres Valero[1]
Fabian Andrés Medina Becerra[2]
Miguel Ángel Mendoza Moreno[3]

[1]Ingeniero Electrónico, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia. Email: ricardo.torres01@uptc.edu.co

[2]Estudiante de Doctorado en Ingeniería. Magíster en Seguridad Informática, Universidad Pedagógica y Tecnológica de Colombia, Sogamoso, Colombia. Email: fabian.medina@uptc.edu.co

[3]Doctor en Ciencias de la Electrónica, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia. Email: miguel.mendoza@uptc.edu.co

Tipo de artículo: Reflexión.
Recibido: 26–09–2019.
Revisado: 02–05–2020.
Aprobado: 05–06–2020.
Doi: 10.21500/20275846.4307

Referenciar así:
R. A. Torres-Valero, F. A. Medina-Becerra and M. A. Mendoza-Moreno, "Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA," *Ingenierías USBMed*, vol. 11, no. 2, pp. 62–70, 2020.

Disponibilidad de datos:
todos los datos relevantes están dentro del artículo, así como los archivos de soporte de información.

Conflicto de intereses:
los autores han declarado que no hay conflicto de intereses.

Editor: Andrés Felipe Hernández. Universidad de San Buenaventura, Medellín, Colombia.

Resumen. La información de una empresa es considerada en la actualidad como uno de los factores más importantes correspondientes a su competitividad. El uso de sistemas de automatización que permitan la supervisión y el control y adquisición de datos (SCADA, del inglés Supervisory Control And Data Acquisition) son necesarios. Las organizaciones emplean este tipo de sistemas para mejorar no solo la eficiencia y eficacia en los procesos, sino adicionalmente para cuidar su seguridad industrial, denotando que con la competitividad acrecentada también se presentan de manera consecuente riesgos que ponen en peligro el actuar de la organización. Dada esta situación, el presente documento pretende, de manera generalizada, exponer un método para guiar el proceso de inspección, con el objetivo de mitigar el riesgo en el área operativa de la organización. Se reconoce que el área administrativa cuenta en la actualidad con un significativo número de programas y metodologías que la han establecido como segura. En este contexto, el avance investigativo condujo a proponer un método de carácter cuantitativo y cualitativo a partir de técnicas de revisión bibliográfica, evocando principalmente la ocupación de ecuaciones de búsqueda.

Palabras Clave. Ciberseguridad, método, riesgo, SCADA, vulnerabilidad.

Abstract. The information of a company is currently considered as an important factor of its competitiveness, so the use of automation systems that allow the Supervisory Control And Data Acquisition (SCADA) are required. Organizations use this type of systems to improve not only the efficiency and effectiveness of the processes, but also to take care of their industrial safety, indicating that with the increased competitiveness there are also consequently risks that jeopardize the actions of the organization. Given this situation, the present document intends to present a method to guide the inspection process, in order to mitigating the risk in the operational area of the organization. It is recognized that its administrative area currently has a significant number of programs and methodologies that have established it as safe; in that context the research progress led to propose a quantitative and descriptive method, based on literature review techniques, mainly evoking the occupation of search equations.

Keywords. Cybersecurity, Method, Risk, SCADA, Vulnerability.

I. Introducción

SCADA, acrónimo de Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de Datos), es conceptualizada como la abstracción respecto a los procesos de monitoreo y control de sistemas industriales. Concretamente el sistema SCADA permite que un operador logre realizar procesos industriales tales como ajustes y cambios, al igual que paradas de emergencia y arranque de equipos desde una estación de programación remota a través de una interfaz amigable, permitiendo una integración hombre maquina [1]. Los sistemas SCADA se desarrollaron para trabajar en redes siempre aisladas, por lo que la seguridad de la información nunca le dio importancia. Sin embargo, durante los últimos años, estos sistemas se han venido integrando a la misma red física de las redes de TI (Tecnología Informática) y a campos como la IoT (Internet of Things) en procesos industriales que tienen rápido crecimiento, permitiendo mayor flexibilidad y conectividad entre dispositivos y sensores [2]. Estas integraciones logran reducir costos de instalación y posibilitan la conexión desde fuera de la empresa, ya sea para generar control de rutina, gestión de alarmas o simplemente soporte técnico.

Los sistemas SCADA, dependiendo de la industria donde se encuentren desplegados, pueden ser considerados como parte de la infraestructura crítica de un país, dependiendo de la relevancia que tenga la industria en la economía. Este tipo de sistemas ha venido siendo objetivo de una gran cantidad de ataques. En el reporte analizado por Gorenc y Sands [3] se identificaron por lo menos 250 vulnerabilidades asociadas a estos sistemas entre 2015 y 2016, mientras que en 2018 el 50% de las computadoras del sistema de control industrial (ICS, Industrial Control Systems) en el sector energético se vio afectada por ataques informáticos [4]. Todo esto genera una preocupación constante entre aquellas empresas que cuentan con este tipo de plataformas para la automatización de los procesos operativos. Así, es posible identificar que la mayor cantidad de necesidades industriales presentes en la sociedad actual son suplidas por SCADA, razón por la cual se han propuesto gran cantidad de iniciativas que permitan conocer los problemas asociados a estos sistemas y de paso se subsanen. Concretamente se logra identificar que los problemas están asociados a la corrupción de la memoria, a credenciales de administración débiles y a métodos de autentificación superficiales, entre otros. De esta manera se logra entender la vulnerabilidad del sistema y las consecuencias de tipo económico, social e inclusive político de la baja seguridad de este sistema. Teniendo en cuenta a Sánchez, Gómez y Cilleruelo [5] es necesario considerar que los problemas se podrían solucionar si las auditorias del sistema fuesen realizadas con un tiempo prudencial y a partir de prácticas seguras de desarrollo. También se afirma que los problemas relacionados con SCADA tienen mucha relación con el diseño de software que no se ha planificado para generar seguridad y bienestar, pues las actualizaciones en su mayoría son simples modificaciones a la interfaz gráfica. Cabe anotar que otro problema asociado a los sistemas SCADA está relacionado con la demora de los fabricantes en resolver un problema de seguridad. Sánchez, Gómez y Cilleruelo [5] consideran que es necesario implementar prácticas de seguridad, debido a que las tecnologías en la actualidad se encuentran mayormente interconectadas, razón por la cual SCADA debe prever cualquier tipo de vulnerabilidad desde cualquier lugar del mundo.

En la actualidad se ha demostrado la importancia que han tenido los sistemas de seguridad y la logística relacionada con las Tecnologías de la Información y la Comunicación (TIC). En este sentido es necesario considerar a los sistemas SCADA como elementos esenciales para la eficiencia y optimización de procesos industriales. Por tal razón, llevar a cabo una auditoría relacionada con este sistema mostrará en primera medida las características primordiales mediante las cuales se genera la implementación del proceso de seguridad, al igual que sus principales fallos y formas de combatir vulnerabilidades.

Consecuentemente, al aplicar una auditoría de ciberseguridad se generará una oportunidad para subsanar las necesidades de seguridad que tienen las organizaciones, presentando una alternativa confiable y fruto de una investigación consistente. Dada esta situación, se propone un método para la auditoría de ciberseguridad aplicable a un sistema SCADA. Para ello es necesario medir, revisar y analizar las diferentes metodologías de seguridad de la información relacionadas con sistemas SCADA, compilar las características que satisfagan las necesidades de seguridad para los SCADA de las metodologías analizadas, caracterizar los activos de la organización y los riesgos asociados al sistema SCADA y finalmente generar y proponer criterios para la propuesta del método de auditoría basado en los resultados obtenidos.

Según el Departamento de Seguridad Nacional de los Estados Unidos [6], la infraestructura crítica puede considerarse como aquella cuyos activos, llámense sistemas o redes, virtuales o efectivos, se reconocen como vitales para un país, dado que su incapacidad o destrucción conduciría a un efecto devastador sobre la seguridad física, económica e inclusive social. Debido a su importancia, es preciso estar al tanto de su seguridad todo el tiempo, evidenciando de esta manera la necesidad de evaluar la vulnerabilidad operacional.

La evaluación de vulnerabilidad operacional y de activos por sus siglas en inglés OCTAVE (Operationally Critical Therat, Asset an Vulnerability Evaluation), de-

sarrollada en el año 2001 por la Universidad de Carnegie Mellon, es una metodología de análisis de riesgos que busca esencialmente facilitar la evaluación de riesgos que tiene una entidad. Esta estudia los riesgos a partir de tres criterios básicos: confidencialidad, integridad y disponibilidad. El sistema es ampliamente usado por el Departamento de Defensa de los Estados Unidos, debido a que posibilita la comprensión del manejo de los recursos y la identificación y evaluación de los riesgos que afectan la seguridad interna de la entidad. Esto requiere llevar a cabo la evaluación de la entidad y del personal de tecnologías de la información [7].

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica (Gobierno de España), es una metodología considerada como uno de los componentes esenciales de las buenas prácticas en el ámbito gubernamental. Su última versión data del 2012 y está perfectamente estructurada a partir de tres guías prácticas. Esta se basa en los activos de la organización y en cinco pasos para realizar el análisis de riesgo [8]. Si bien no se comporta como una metodología específica para SCADA, se ocupa de la gestión del riesgo de la información. Por tanto, la norma suministra directrices claras sobre la gestión de riesgos de seguridad para una empresa concreta. Sin embargo, es aplicable a todo tipo de organizaciones que cuenten con la intención de gestionar los riesgos asociados con la ciberseguridad de la organización y no especifica un procedimiento concreto dado a que esto depende de factores asociados directamente con las condiciones de la organización en particular [9].

Establecer formas para mejorar la seguridad en sistemas SCADA es una preocupación que ha aparecido constantemente en las investigaciones de tipo informático. Es el caso de la investigación realizada por Alves, Das, Werth y Morris [10], en la cual se hace referencia a las amenazas potenciales cuando los desarrolladores y las empresas utilizan SCADA como una forma de potenciar infraestructuras críticas sin tener en cuenta la seguridad como factor esencial. Existen diferentes tipos de ataques que pueden ocurrir en cualquiera de las capas de operación de la organización, desde el nivel de supervisión hasta el nivel de los equipos de instrumentación, donde atacan al hardware, al software y a la conexión de red [11]. Incluso se encuentran ataques dirigidos a través del motor de búsqueda Shodan, en donde los atacantes de manera regular encuentran un camino sustancial para generar daños en los procesos que se llevan a cabo al interior de las empresas. Gracias a la base de datos de Shodan es posible acceder a más de 500000 dispositivos de los principales fabricantes de SCADA y evaluar sus vulnerabilidades mediante minería de texto y minería de datos. Se evidencia que miles de estos dispositivos tienen credenciales de fabrica o software desactualizado [12] y a partir de la investigación referida se ha podido concretar que el sistema es bastante endeble. Así mismo, en la investigación realizada por Sevillano y Beltrán [13], se menciona a MAASERISv2.1 (Metodología para el Análisis, Auditoría de seguridad y Evaluación de Riesgo operativo de redes Industriales y sistemas SCADA), que ya se encuentra en su versión 3.0, pero de la cual existe poca información pública debido a que es propiedad de Logitek.

Por lo tanto, como primer paso para implementar avances en el sector de la ciberseguridad se requiere el uso de diferentes formas de analizar el impacto sobre los sistemas que en la actualidad están en auge. Así pues, para el análisis de estas características es primordial establecer un método que tenga en cuenta los entornos de operación de SCADA. Como resultado relevante del estudio, se promueve un método para realizar una auditoría a SCADA y se pone de manifiesto la necesidad de trabajar con el análisis de activos de la organización, la identificación de vulnerabilidades y la gestión del riesgo operativo.

Con el fin de trazar el avance de las metodologías necesarias para minimizar los problemas con SCADA, se hace necesario referenciar el documento de Arias [14] titulado “Riesgos a los Sistemas SCADA, en empresas Colombianas”. Este tiene como objetivo identificar de manera clara cuales son los principales riesgos que se asocian a la globalización y a la ocupación de sistemas como SCADA. Su hallazgo principal es, al momento de instaurar este sistema como completamente funcional en una empresa, establecer en primera medida y de manera correcta la estimación de recursos que serán ocupados tanto en el presente como en el futuro y, en el mismo sentido, plantea como una necesidad tomar los modelos de aplicación que se encuentran en otros países.

Finalmente, Ghosh y Sampalli [11] enumeran todos los estándares actuales que usan las organizaciones para la infraestructura de comunicaciones SCADA y detectan como principales amenazas de seguridad la falta de defensa contra ataques de denegación de servicios (DoS, Denial of Service) y el uso de protocolos débiles para el intercambio de claves. Por otro lado, Anabalón y Donders [15] referencian directamente a Ethical Hacking como un método claro que garantiza la seguridad de los Sistemas IT y plantean generar como forma de mitigación del riesgo un *Escáner nmap*, que son planes de contingencia e incremento de la seguridad industrial. Es así como en diferentes pruebas, en las cuales se representaba una acción real de ataque, se mostraba que los sistemas SCADA son muy endebles, situación por la cual se presentan gran cantidad de problemas asociados con el funcionamiento normal de una organización. En general, se identifica que son muchos los sectores que pueden verse realmente afectados cuando existe una intromisión en el sistema.

II. Materiales y métodos

La presente investigación se enmarca en un estudio de carácter cuantitativo y descriptivo, dado que recolecta, mide y evalúa información relevante acerca de las variables de estudio o conceptos que se han construido acerca de ellas. Según [16] el estudio cuantitativo limita la idea, para así extraer objetivos y preguntas que construyan un método teórico al revisar la literatura, mientras que el estudio descriptivo es ideal para revisar con precisión las dimensiones del contexto a estudiar. De esta manera es consecuente afirmar que para el desarrollo de la investigación fue necesario considerar las siguientes ecuaciones de búsqueda que coadyuvaron de manera significativa a encontrar la información para determinar los principales resultados investigativos. Entre las principales ecuaciones es posible especificar las que combinan SCADA y Metodología, SCADA y Ciberseguridad, SCADA y Riesgo, SCADA y Vulnerabilidad, limitando la revisión a publicaciones realizadas desde el año 2012.

Teniendo en cuenta la metodología propuesta, se logra especificar en primera medida los diferentes riesgos a los que se encuentran expuestos los sistemas de producción de las organizaciones, evidenciando el poco interés que se le ha prestado antes a esta área. Del mismo modo se logra concertar la ocurrencia de los hechos, la severidad y la detección de los mismos a través de su producto en el Índice de Riesgo Interno –en adelante |R|–, que facilita el trabajo de medición del riesgo operativo y permite identificar y analizar vulnerabilidades potenciales y sus efectos, además de reconocer acciones que mitiguen o eliminen la posibilidad de este riesgo.

El proceso de seguridad pretendido debe conciliar su aplicación tanto en el área operativa como en el área administrativa, es por esta razón que en una parte del ciclo se presenta la conjunción entre ambas.

III. Resultados

Cuando se precisa analizar el concepto de ciberseguridad, específicamente el que se incluye en el ámbito de la seguridad industrial, se entiende que la información, los sistemas o las instalaciones deben ser protegidos de peligros externos tales como ataques o amenazas que se originen desde medios tecnológicos. De esta manera, el diseño de los programas que estén destinados a mejorar la seguridad deben proveer una confidencialidad adecuada, además del uso de protocolos específicos [9]–[12].

Con respecto a la implementación de sistemas de seguridad al interior de las empresas, es conveniente señalar que estas se están organizando tecnológicamente para disminuir las amenazas desde el ámbito administrativo, mas no desde el ámbito operativo. Esto las hace vulnerables, dado que en los últimos años este sector se ha visto realmente amenazado con el surgimiento de diversas formas de APTs (Advanced Persistent Threat), tales como Stuxnet, Shamoon, Sandworm o Duqu, que son acciones relacionadas con el cibercrimen y ciberterrorismo. De hecho, la intención que se evidencia en el mundo, basada en proteger los sistemas administrativos y operativos, parte de los ataques sistemáticos que han sufrido los sistemas SCADA.

Adicionalmente, es preciso afirmar que dada la integración que han tenido los sistemas administrativos y operativos, se produce una amenaza al interior del sistema operativo. Sin embargo, el entorno no permite que se genere una protección al sistema operativo, como si ocurre con el sistema administrativo. En la Tabla 1, aportada por Sevillano y Beltrán [13], se vislumbra la necesidad diferenciada de procesos de seguridad industrial:

Teniendo en cuenta los riesgos a los que se enfrenta el Operation Technology (OT), es preciso detallar que son muchas las metodologías que se han desarrollado para mejorar la seguridad en el sistema SCADA, sin embargo, la mayoría de estas metodologías son puramente diseñadas para el ámbito administrativo sin tener en cuenta el diseño de software para la protección del ambiente operativo de la empresa. De hecho, se logra especificar que las metodologías son explícitamente diseñadas para evaluar los riesgos que se consideran estratégicos, de ese modo no tienen en cuenta la operacionalidad de la empresa, que es un ámbito que también se encuentra en suficiente riesgo [13].

Para dar un ejemplo de este tipo de metodologías, es preciso nombrar a la IT-Grundschutz (IT Baseline Protection) [17] que, siendo utilizada por el Ministerio del Interior Alemán, ha logrado disminuir los riesgos en las organizaciones tipificadas como críticas, en donde se evalúa consecuentemente la parte corporativa o estratégica, dejando de lado los riesgos operativos. Tal entorno es conveniente, pues hace un análisis de los factores físicos y lógicos en donde se relaciona de manera directa el entorno organizacional, extendiendo el análisis a la dependencia entre factores y analizando amenazas o vulnerabilidades que puedan tener orígenes disímiles, tales como desastres naturales, errores y fallos no intencionados o deliberados, que puedan poner en peligro la organización.

Cuando se trata de establecer las principales normas y prácticas para mejorar la seguridad al interior de la organización desde el ámbito operativo, es preciso nombrar las detalladas por el ICS CERT del Departamento de Seguridad Nacional de los Estados Unidos y las realizadas por el CPNI del Gobierno del Reino Unido acerca de cómo aumentar la seguridad de los sistemas de control industrial frente a ataques informáticos. Así, se destaca la aproximación generada por el National Institute of Standard Technologies (NIST) para la elaboración de programas en gestión de parches, el conjunto de normas ISA99, creadas por la Inter-

Tabla 1. Diferencias entre ciberseguridad administrativa y operacional.

Ámbito administrativo	Aspecto	Ámbito operacional
Confidencialidad, integridad y disponibilidad.	Objetivo	Disponibilidad, integridad y confidencialidad.
2 a 3 años con la existencia de gran número de proveedores.	Ciclo de vida.	10 a 20 años con un reducido número de proveedores específicos.
Práctica habitual que conduce inversión en ciberseguridad.	Evaluación cuantitativa del riesgo	Práctica realizada si es obligatoria.
Habitual e integrado en la operación.	Desarrollo de sistemas de gestión de la seguridad.	No habitual y no integrado.
Común, fácil de actualizar y con políticas bien definidas y automatizadas.	Antivirus y parches.	Poco habitual por la criticidad de los sistemas, complejo de desplegar y actualizar.
Normativas genéricas	Cumplimiento de normativas	Normativas específicas y/o sectoriales.
Utilización de las metodologías estándares más actuales.	Testeo y auditorías.	Test específicos e inexistencias de metodologías estándares.
Fácil despliegue y en ocasiones de carácter obligatorio.	Respuesta a incidencias y análisis forense.	Poco habitual y sin análisis forense.

Fuente: Sevillano y Beltrán [13]

national Society of Automation (ISA) o la realizada por Sandia National Laboratories sobre Penetration Testing en sistemas de control industrial. Adicionalmente, la metodología desarrollada por el Department of Homeland Security (DHS), que ayuda a establecer el nivel de adecuación de un entorno industrial con respecto a estándares predefinidos por las NIST y la Norh American Electric Reliability Corporation (NERC) a través de la aplicación conocida como Cyber Security Evaluation Tool [15], [18]. El Gobierno de los Estados Unidos y el Gobierno británico han promovido y desarrollado tecnologías a partir de Blockchain para asegurar las ICS del sector de energía. Además, generan herramientas para proteger la confidencialidad encriptando la información y se estandariza la tecnología IoT con contratos inteligentes para prevenir el phishing haciendo uso del correo electrónico con registros inmutables [11].

En el análisis de estas metodologías y normas es preciso considerar que la mayoría de aproximaciones tienen como fin la identificación de los riesgos o vulnerabilidades asociadas a los sistemas más frecuentes en los entornos operativos. Si bien las metodologías y normas denotadas con anticipación promueven un análisis exhaustivo, se precisa que no se cuente con una metodología que mejore de manera considerable las condiciones holísticas de la organización, exponiendo un método que proteja al sistema operativo de la empresa [17], [19]. Por esta razón, se expone a continuación una propuesta de método adaptada al ámbito industrial, en donde se identifican los activos que se han vinculado a los entornos operativos, además de las principales variables que provocan vulnerabilidad asociada y que permiten la gestión del riesgo operativo.

La información que se presenta a continuación puede integrar a otras metodologías y métodos que beneficien la seguridad del ámbito organizacional y operativo. En este sentido, se considera un complemento a metodologías y métodos específicos de evaluación de riesgos estratégicos en infraestructuras críticas. Según Sevillano y Beltrán [13] una metodología para el análisis, auditoría de seguridad y evaluación de riesgo operativo de redes industriales y sistemas SCADA se considera como un conjunto de procesos, herramientas y entregables que permiten analizar el estado que tiene una red industrial desde el análisis de la seguridad. Esto permite la evaluación de la disponibilidad y facilita un profundo análisis de las principales condiciones que presentan vulnerabilidad en el entorno operativo. Además, proporciona una evaluación cuantitativa del riesgo operativo, pues sirve como documentación complementaria y útil para el desarrollo de los planes de seguridad del operador y los planes de protección específicos.

Se determinan cuatro áreas específicas de observación para el diseño del método, en donde se encuentran consignadas el ciclo de análisis de activos, la identificación de amenazas y vulnerabilidades, la evaluación del riesgo operativo y las medidas de protección [7]–[9], [13], [18]. En la Figura 1 se detallan los principales retos que tiene el método.

En principio se requiere realizar el análisis de activos donde se deben identificar, clasificar y valorar aquellos que han sido vinculados al entorno operativo, para esto se debe evidenciar una base de datos que facilite la introducción de la clasificación de los activos de la organización y la dependencia que existe entre estos [8], [13], [20]. Para nombrar algunos tipos de activos se presenta el siguiente listado:

- Datos.
- Servicios.
- Aplicaciones informáticas.
- Equipos de cómputo.
- Controladores, electrónica de potencia, maquinaria.
- Firewall/UTM (Unified Threat Management).
- HMI (Human-Machine Interface)/Panel Táctil.
- Personal, entre otros.

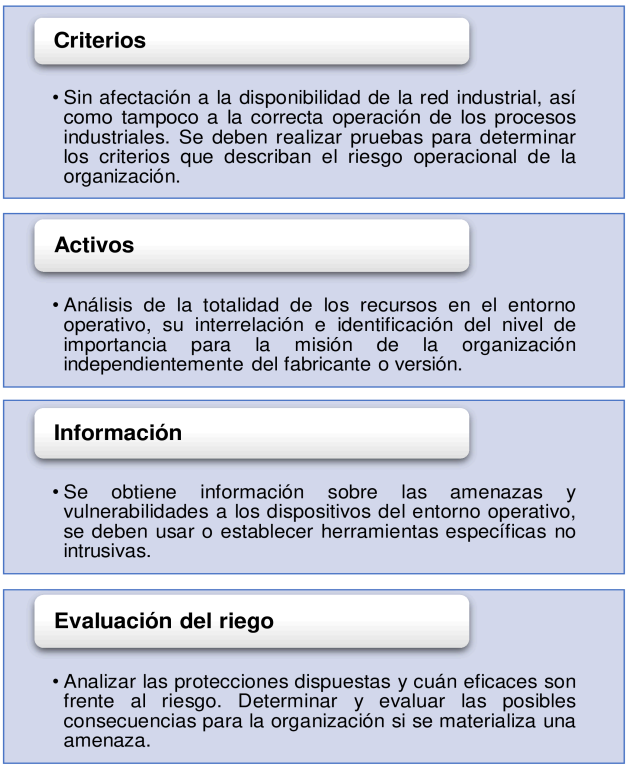

Figura 1. Retos para el diseño del método. Fuente: Autores

Una vez se definen los activos desplegados es preciso realizar una agrupación física, técnica y de recursos humanos, comprendiendo entonces categorías como edificio, sala, rack, hardware, software, redes lógicas y físicas, dependencias o departamentos, entre otras. Después de ello se debe realizar un análisis de la identificación de las amenazas y vulnerabilidades a través de diferentes técnicas y herramientas que han sido expuestas por Shodan, Kali Linux, Network Security Toolkit (NST), Bugtraq y Nessus. Aquí se descubren las diferentes amenazas y vulnerabilidades que se asocian con los activos y con las agrupaciones de los mismos [12], [19]. Es importante solo usar herramientas que no sean intrusivas en el entorno operativo.

Para denotar las principales amenazas y vulnerabilidades se muestra a continuación una clasificación según el ámbito en el que eventualmente se presentan, de este modo es preciso considerar la seguridad física, la seguridad política y la seguridad del proceso operativo. Es importante identificar y valorar cada amenaza y vulnerabilidad para caracterizar el entorno al que se enfrenta el sistema SCADA, incluyendo dentro de este análisis la tolerancia a fallos, la disponibilidad, la visibilidad, el acceso entre redes, la criptografía, entre otras. Adicional a ello, la tercer área de análisis es la evaluación del riesgo operativo, en esta se tiene en cuenta la posibilidad de riesgo que es vinculado a la producción de la empresa. El riesgo que se plantea mitigar afectaría de manera directa al personal, los procesos, los sistemas y la tecnología de la organización.

Realizado el análisis de activos e identificación de amenazas y vulnerabilidades se procede a calcular el |R| que, como se mencionó anteriormente, se calcula multiplicando los factores ocurrencia, severidad y detección.

La ocurrencia definida como la probabilidad del riesgo en aparecer tiene una determinación compleja y difiere de forma cualitativa y cuantitativa entre metodologías existentes, se deberá valorar del 1 al 5 y de acuerdo a [7], [9], [13], [18] se crea el siguiente listado:

1. El riesgo es extremadamente difícil de manifestarse (siglos).
2. El riesgo es muy difícil de manifestarse (décadas).
3. El riesgo es posible de manifestarse (anual).
4. El riesgo se manifiesta frecuentemente (mensual).
5. El riesgo es casi seguro de manifestarse (diario).

Ahora bien, en cuanto a la severidad, esta indica la gravedad de los efectos que traería la aparición del riesgo, en este sentido afecta de manera directa la disponibilidad, integridad y confidencialidad de los objetos de análisis. Esta al igual que la ocurrencia debe valorarse de 1 a 5. Basado en [7], [13], [18] se generan los siguientes criterios:

1. El riesgo no afecta la operación de la organización.
2. El riesgo afecta la operación de la organización, pudiéndose recuperar con protecciones establecidas previamente y sin que afecte el valor de los activos.
3. El riesgo afecta a la operación de la organización, pudiéndose recuperar con protecciones establecidas previamente a una operación básica que cumpla la misión de la organización y sin que afecte el valor de los activos.
4. El riesgo afecta a la operación de la organización, pudiéndose recuperar con protecciones establecidas previamente a una operación básica que cumpla la misión de la organización y afectando el valor de los activos.
5. El riesgo afecta a la operación de la organización, no pudiéndose recuperar.

En consecuencia, es preciso considerar la detección del riesgo que, según los estándares planteados por la severidad y la ocurrencia, también se establece en una escala de 1 a 5. Siguiendo los preceptos mostrados por [7], [9], [13], [18] se produce esta lista:

1. El riesgo siempre es detectable.
2. El riesgo fácilmente es detectable.
3. El riesgo normalmente es detectable.
4. El riesgo difícilmente es detectable.
5. El riesgo no es detectable.

Como se puede identificar, el |R| es de gran utilidad, precisamente porque ayuda a estimar la ocurrencia, la severidad y la detección del riesgo. Adicional a ello, establece la comparación y el ordenamiento de un conjunto de riesgos de mayor a menor, al igual que en sentido contrario. También se establece a partir de ello las prioridades por las que debe velar el sistema, pues su valor estará entre 1 y 125. Este es directamente proporcional al riesgo al que está expuesta la organización.

Con la intención de especificar responsabilidades y escenarios de amenazas para determinar las medidas de protección, es conveniente precisar que se divide la tipología en tres tipos de riesgos: el primer tipo recoge los riesgos netamente técnicos, que son específicos del área operativa; el segundo tipo de riesgos recoge aquellos que si bien pertenecen al área operativa, no son específicos de estas, teniendo en cuenta que en las áreas operativas se presenta cada vez más una inclusión del área administrativa; finalmente la tipología tres recoge los riesgos políticos y legales a los que se enfrenta la organización, estos, a pesar de pertenecer al área administrativa, realizan modificaciones al área operativa, en donde funcionan algunos tipos de políticas y normatividades legales [13]. Teniendo en cuenta estas tres tipologías se determinan algunas relaciones para priorizar y generar medidas de protección [7], [9], [18] –incluidas en la Figura 2–.

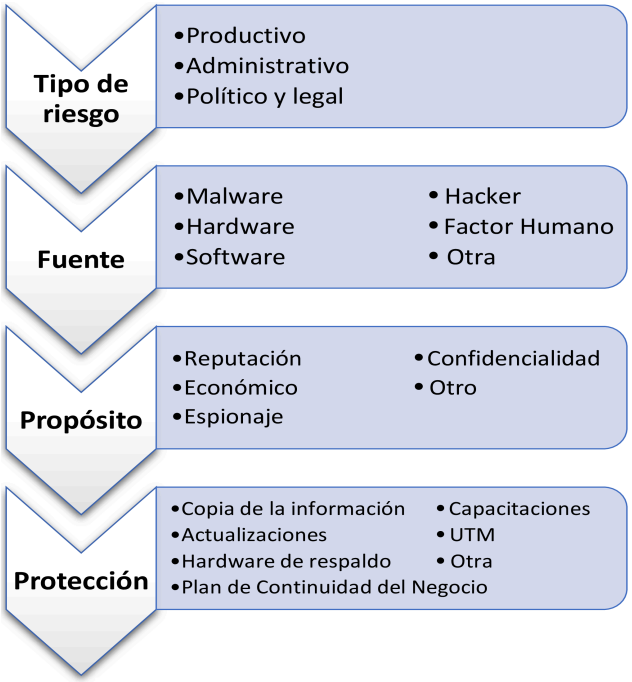

Figura 2. Tipos de riesgo y relaciones. Fuente: Autores

Para finalizar, es preciso considerar que el método expuesto requiere que se lleven a cabo en su conjunto las etapas que detalla la Figura 3:

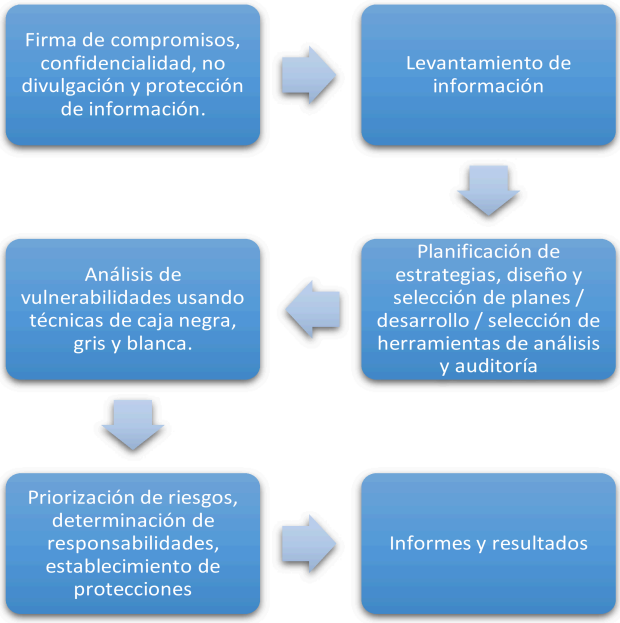

Figura 3. Proceso de implementación. Fuente: Autores

Los encargados de la auditoría deben presentar los documentos que se detallan a continuación:

1. Resumen ejecutivo.
2. Inventario y dependencia entre activos.
3. Arquitectura de operación.
4. Mapa de arquitectura de operación.
5. Informe de vulnerabilidades.
6. Informe de riesgos.
7. Mapa de riesgos y seguridad.
8. Medidas de seguridad/Protecciones recomendadas.
9. Políticas y procedimientos de seguridad.

IV. Conclusiones

En el presente documento se realizó un análisis de los sistemas SCADA, denotando la gran acogida que estos tienen al interior de cualquier organización, sin embargo, se resalta que dado el contexto en el que son funcionales se presentan eventualmente gran cantidad de riesgos que son parte tanto del área administrativa, como del área operativa, reconociendo que los primeros han sido estudiados de manera amplia y por tanto se hace necesario abordar los riesgos que se generan en los segundos, aportando innovación y granularidad para preservar su integración con la seguridad administrativa.

Una vez se define el problema que suscita la falta de protección de los sistemas SCADA, las principales motivaciones para establecer un cambio sustancial en la forma en que se está dando la protección del entorno y evocando los principales conceptos que se anidan

alrededor de este proceso, se realiza una especificación de las principales metodologías que han sido expuestas hasta el momento, para con ello tener una base que promueva el método ajustado al estudio y el contexto de las organizaciones.

A partir del método propuesto es preciso establecer las principales vulnerabilidades a las que se encuentran expuestos los entornos de producción y reconocer las mejoras prácticas que expone la evaluación del riesgo. Así mismo, las mejores prácticas que se deben establecer y los activos y grupos en los que se clasifican estos mismos. Por lo tanto, se definen tres áreas de análisis que son: los activos, las vulnerabilidades y la gestión del riesgo operativo, en donde se establece un ciclo del desarrollo de análisis y auditoría que incluye documentos entregables en donde se evidencia el proceso de seguridad.

Se espera que con la puesta en marcha del método propuesto se mejore considerablemente la seguridad en el área operativa de cualquier organización y se evidencie de esta manera una mitigación de los peligros inminentes para las empresas.

V. Trabajos futuros

Se plantea como trabajo futuro la necesidad de aplicar el método propuesto, a fin de cuantificar su eficiencia.

Referencias

[1] G. Tiburski, G. T. Moreira, and M. Misagui, "Supervisory Systems integration SCaDA and ERP for production control in real time," *Revista Espacios*, vol. 38, no. 4, p. 5, 2017.

[2] B. Sánchez Torres, J. A. Rodríguez Rodríguez, W. Rico Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," *Revista Facultad de Ingeniería*, vol. 27, no. 47, pp. 93–101, 2018.

[3] B. Gorenc and F. Sands, "Hacker Machine Interface: The State of SCADA HMI Vulnerabilities," TrendLabs Research Paper, 2017. [Online]. Available: https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf.

[4] T. R. Vance and A. Vance, "Cybersecurity in the Blockchain Era : A Survey on Examining Critical Infrastructure Protection with Blockchain-Based Technology," IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, pp. 107–112, 2019. doi:10.1109/PICST47496.2019.9061242.

[5] M. Sánchez Rubio, J. M. Gómez-Casero and C. Cilleruelo Rodríguez, "Inseguridad en infraestructuras críticas," de *Jornadas Nacionales de Investigaciíon en Ciberseguridad (1a. 2015. León),* León, 2015.

[6] S. Pagnotta, "Ataques a infraestructuras críticas, ¿modalidad inminente en 2017?," 2017. [Online]. Available: www.welivesecurity.com/la-es/2017/01/04/ataques-a-infraestructuras-criticas-2017.

[7] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," *Procedia Computer Science*, vol. 135, pp. 202–213, 2018.

[8] F. Y. Holguín García and L. M. Lema Moreta, "Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies," de *2018 7th International Conference On Software Process Improvement (CIMPS)*, Guadalajara, Jalisco, Mexico, 2018.

[9] Consejo Superior de Administración Electrónica, "MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información," 2012. [Online]. Available: administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XV8RLuj0nIV.

[10] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of SCADA testbeds for cybersecurity research: A modular approach," *Computers & Security*, vol. 77, pp. 531–546, 2018.

[11] S. Ghosh and S. Sampalli, "A Survey of Security in SCADA Networks: Current Issues and Future Challenges," in *IEEE Access,* vol. 7, pp. 135812–135831, 2019. doi: 10.1109/ACCESS.2019.2926441.

[12] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly, and H. Chen, "Identifying SCADA Systems and Their Vulnerabilities on the Internet of Things: A Text-Mining Approach," *IEEE Intelligent Systems*, vol. 33, no. 2, pp. 63–73, 2018.

[13] F. Sevillano and M. Beltrán, "Metodología para el Análisis, Auditoria de Seguridad y Evaluación del Riesgo Operativo de Redes Industriales y Sistemas SCADA (MAASERISv2.1)," de *Jornadas Nacionales de Investigación en Ciberseguridad (1a. 2015, León)*, León, 2015.

[14] J. E. Arias Torres, "Riesgos a los sistemas SCADA, en empresas colombianas," Trabajo de grado, Universidad Piloto de Colombia, Bogotá, 2014.

[15] J. Anabalon y E. Donders, "Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001–2005", de MonkeysLab Research, Universidad de Santiago de Chile, Departamento de Ingeniería Informática, Chile, 2014.

[16] R. Hernández Sampieri, C. Fernández Collado, and M. D. P. Baptista Lucio, *Metodología de la Investigación,* vol. 6. Mexico: McGRAW-HILL, 2014.

[17] S. Bergner and U. Lechner, "Cybersecurity Ontology for Critical Infrastructures," in Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering

and Knowledge Management–Volume 2: *KEOD*, pp. 80–85, 2017.

[18] K. Stouffer, V. Pillitteri, M. Abrams and A. Hahn, *Guide to Industrial Control Systems (ICS) Security*, NIST.SP.800-82r2, 2015.

[19] S. Samtani, S. Yu, H. Zhu, M. Patton and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," de 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, 2016.

[20] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek and A. Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," in Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14), Aug. 2014.