TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.47-53 ISSN 1729-3804

# ESTRATEGIA DE CIBER SEGURIDAD PARA LA SOCIEDAD DIGITAL

**Lesly Núñez Jarrosay**

Empresa de Tecnologías de la Información para la Defensa, XETID, Calle 296 entre Ave. 207 y 203.Boyeros, La Habana, Cuba.
lnunez@xetid.cu

**RESUMEN**

En los últimos años, las tecnologías de la información han evolucionado de manera exponencial, la tendencia a la informatización y la conectividad de todo tipo de objetos ha marcado un hito en el desarrollo de esta era. Pero lamentablemente en muchas ocasiones los sistemas de gestión de seguridad se han quedado estancados en el pasado. En el siguiente trabajo se describen las tendencias de la sociedad digital actual y las carencias de los sistemas de seguridad que se emplean con respecto a las características que demanda el avance en el proceso de informatización. Se explica cómo las soluciones más completas como los Sistemas de Gestión de Información y Eventos de Seguridad, hoy en día requieren de una actualización que les permita gestionar el gran volumen de datos que se genera en las redes modernas. Se describen requisitos como la gestión de big data, la necesidad de aprendizaje automático o machine learning, la exigencia de que estos sistemas desarrollen análisis del comportamiento de entidades y usuarios y cómo cada uno de estos conceptos incrementa la confiabilidad de la información de seguridad que se obtiene de las aplicaciones que los emplean. Se presentan además los principios que se han adoptado para el desarrollo de una plataforma de seguridad de nueva generación que permita garantizar un mayor índice de éxito en la detección y prevención de las amenazas cada vez más sofisticadas, que surgen y se desarrollan a partir de la evolución de la era digital.

**PALABRAS CLAVES:** Ciberseguridad, era digital, BIG DATA, Next-Gen SIEM.

# CYBER SECURITY STRATEGY FOR THE DIGITAL SOCIETY

**ABSTRACT**

In recent years, information technologies have evolved exponentially, the trend towards computerization and the connectivity of all kinds of objects has marked a milestone in the development of this age. But unfortunately on many occasions security management systems have been stagnant in the past. The following work describes the trends of today's digital society and the lack of security systems that are used with respect to the characteristics demanded by the progress in the computerization process. It explains how the most complete solutions such as Security Information and Events Management systems, today require an update that allows them to manage the large volume of data generated in modern networks. Requirements such as big data management, the need for machine learning, the requirement that these systems develop an User and Entity Behavior Analytics are described, also how each of these concepts increase the reliability of the security information that gets from the applications that use them. It also presents the principles that have been adopted for the development of a new generation security platform that ensures a higher success rate in the detection and prevention of increasingly sophisticated threats that arise and develop from the Evolution of the digital age.

**INDEX TERMS:** Cyber security, digital age, BIG DATA, Next-Gen SIEM.

## 1. INTRODUCCIÓN

Hasta hace unos años las estrategias de seguridad de las redes eran suficientes aun cuando solo contaban con herramientas distribuidas, tales como cortafuegos, IPS/IDS, antivirus, entre otras. Con el paso del tiempo fue preciso emplear sistemas que unificaran la información obtenida, que generaran alarmas y reportes más eficientes y que

Manuscrito recibido: 2020-10-05, aceptado: 2020-12-04
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

correlacionaran los datos obtenidos. Lo anterior dio paso al surgimiento de los sistemas de Gestión de Información y Eventos de Seguridad, SIEM.
Un sistema SIEM proporciona una consola central para ver, monitorear y administrar eventos relacionados con la seguridad y datos de registro de toda la empresa. Debido a que se correlaciona datos de múltiples fuentes, un sistema SIEM puede permitir que un analista identifique y responda a patrones de comportamiento sospechoso más rápido y más eficazmente de lo que sería posible mirando datos de sistemas individuales [1].
Las plataformas SIEM combinan los conceptos de Security Information Management (SIM) y Security Event Management (SEM). El primero se centra en el análisis y la presentación de informes de datos de registro y el almacenamiento a largo plazo, mientras que el segundo se centra en el monitoreo y las notificaciones en tiempo real. SIEM incluye además el análisis y la correlación en tiempo real [2].
Según la consultora Gartner el mercado de Gestión de Eventos e Información de Seguridad (SIEM) surgió por la necesidad del cliente de analizar los datos de eventos en tiempo real para la detección temprana de ataques dirigidos y violaciones de datos, además de recopilar, almacenar, investigar e informar sobre archivos de registro para dar respuesta a incidentes, análisis forense y cumplimiento normativo [3]. La tecnología SIEM agrega datos de eventos producidos por dispositivos de seguridad, infraestructura de red, sistemas y aplicaciones. La fuente de datos primaria son los datos de registro, pero también puede procesar otras formas de datos, como la telemetría de red. Los datos de eventos se combinan con información contextual sobre usuarios, activos, amenazas y vulnerabilidades. Estos registros pueden normalizarse, de modo que los eventos, los datos y la información contextual de fuentes dispares puedan analizarse para fines específicos, como el monitoreo de eventos de seguridad de la red, el monitoreo de la actividad del usuario y los informes de cumplimiento [3].
Desde sus inicios los SIEM alcanzaron mucha popularidad hasta convertirse en uno de los mecanismos de seguridad más completos. Hoy en día, con el auge de la era digital, el volumen de datos a procesar ha aumentado considerablemente y los SIEM tradicionales no han sido capaces de gestionar este cúmulo de información de manera eficiente. Es por ello que en el mundo se han implementado nuevas estrategias que permitan aumentar la calidad de la gestión de seguridad a la par que aumentan las opciones de conectividad.
En este trabajo se describirá la necesidad de emplear soluciones SIEM de próxima generación o Next Generation SIEM. En la primera sección se caracterizará la sociedad digital como pilar fundamental del cambio tecnológico. Posteriormente se describirán los motivos y requisitos de los SIEM de próxima generación y finalmente se expondrán los progresos que se han obtenido en el diseño de este tipo de plataformas empleando software libre.

## 2. SOCIEDAD DIGITAL

La sociedad digital ha sido el resultado de un proceso de transformación, el cual integra la tecnología digital en todos los aspectos cotidianos y del negocio y que requiere cambios fundamentales en el ámbito de la tecnología, la cultura, las operaciones y la entrega de valor [2]. Esta sociedad tiende a ser identificada como una consecuencia directa de la consolidación de la sociedad de la información y del conocimiento. [4]. Básicamente se trata de una sociedad, donde las prácticas productivas y comunicativas se realizan fundamentalmente a través medios digitales. Tecnologías como 5G, inteligencia artificial, reconocimiento de la voz, reconocimiento facial, realidad aumentada, realidad virtual, edge computing o cloud computing, se van convirtiendo en habituales, integrándose en el día a día [5].
Para aprovechar mejor las tecnologías emergentes y su rápida expansión en las actividades humanas, los usuarios y las entidades transforman e informatizan todos sus procesos y modelos. La transformación digital implica sustituir la tecnología anterior, que puede ser costosa de mantener para la empresa, y modificar la cultura popular y empresarial de manera que respalde la aceleración que trae consigo este proceso.

## 3. NECESIDAD DE EMPLEAR SIEM DE NUEVA GENERACIÓN

Los SIEM hoy en día van más allá de los dominios clásicos de seguridad y se emplean incluso como sistemas de control de violación de políticas en operadoras telefónicas. Su mercado ha crecido rápidamente, hasta el punto de que la consultora Gartner le dedica un reporte técnico a la comparación entre las diferentes plataformas [6].
Sin embargo, la llegada de la transformación digital introduce nuevos retos en el ámbito de la ciberseguridad debido a que los datos han ganado en variedad, volumen y velocidad. La combinación de la analítica de datos y el Big Data, obliga a introducir un cambio radical en los sistemas SIEM tradicionales [3].
El Big Data se define como un set de datos cuyo tamaño va más allá de lo que una herramienta típica de base de datos puede capturar, almacenar, gestionar y analizar [7]. El volumen de big data en muchos sectores va de decenas de terabytes (TB: aproximadamente $10^{12}$ bytes) a múltiples peta bytes (PB: aproximadamente $10^{15}$ bytes) [7].
Los big data pueden ser de volumen demasiado grande, variar muy rápido o no coincidir con la estructura de las arquitecturas convencionales de bases de datos. Lo anterior introduce el primer reto al que se enfrentan los SIEM tradicionales: El incremento del volumen de datos [8].

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.47-53 ISSN 1729-3804

La cantidad de información de seguridad que generan los dispositivos de computación sigue aumentando, casi todas las acciones que se desarrollan en los mismos genera un log o registro. Por ejemplo, cargar una página web en un dispositivo final como una laptop o una computadora de escritorio, genera múltiples eventos en diversos dispositivos. Por ejemplo el firewall o cortafuegos decide si el paquete puede ser reenviado o si es bloqueado, según las reglas que tenga definidas, igualmente ocurre en el proxy institucional y en el propio dispositivo, donde se registra una nueva conexión y el programa antimalware genera varios logs respecto a la misma [8].

Las tecnologías convencionales a menudo no pueden soportar el análisis primario a gran escala y de gran potencia porque retener un volumen de datos tan grande suele ser caro o poco factible. Por consiguiente la mayoría de los eventos y logs son eliminados luego de un período de tiempo [9]. Además son ineficientes al realizar análisis y consultas en grupos de datos grandes y no estructurados.

Incluso en los casos donde el volumen de datos puede no ser tan grande, las nuevas amenazas emergentes están marcando la necesidad de una evolución en la gestión de seguridad. Las redes de movimiento lateral, o simplemente el movimiento lateral, es una de las últimas técnicas empleadas por los ciber-atacantes para moverse libremente por una red, mientras investigan y obtienen información de la misma para realizar su ataque. Actualmente es una de las mayores amenazas de seguridad en la red y la detección de los paquetes maliciosos tarda aproximadamente 107 días, ya que tienen la capacidad de evadir los métodos de seguridad estáticos [10].

Existen diversos ataques de movimiento lateral y algunos muy eficientes como es el caso de las Amenazas Persistentes Avanzadas (APT Advanced Persistent Threat). Las APT se usan por atacantes muy habilidosos y motivados, con recursos para desarrollar ataques extensos y sofisticados. Se enfocan en un único objetivo por un período extenso de tiempo y continuamente se adaptan a las tácticas defensivas de la víctima para mantener su posición establecida en la red [8].

Las nuevas tácticas, técnicas y procesos desarrollados por los intrusos más avanzados han debilitado la efectividad de métodos de defensa estáticos como los IDS/IPS basados en firmas, debido a que estos no pueden detectar ataques de día cero [8] y son ineficientes en el descubrimiento y la detención de APT u otros ataques de movimiento lateral.

Otro desafío para los SIEM heredados es que los registros no contienen toda la información necesaria para seguir un ataque lateral. Cuando están limitados por la falta de capacidades de seguimiento lateral del SIEM, los analistas tienen que reconstruir manualmente el rastro de ataque, que lleva mucho tiempo, es ineficiente y a menudo ineficaz [4].

Otro de los grandes problemas de los SIEM tradicionales es el nivel de ruido o los falsos positivos [8]. Las reglas del SIEM deben ser creadas y revisadas manual y constantemente para que puedan detectar los incidentes de seguridad. Esto requiere de personal calificado capaz de crear o modificar las mismas [8]. La mala configuración de estas, las alertas o los reportes, puede producir lo que en ciberseguridad se conoce como ruido, que no es más que la generación de alertas sin valor real de seguridad

Teniendo en cuenta lo anterior, cuando se reciben las alertas los analistas deben revisar la información y verificar si es o no un falso positivo para luego actuar en correspondencia. Estas acciones pueden prolongar el tiempo requerido para detectar la amenaza en sí. Los seres humanos tienden a cansarse o perder la concentración cuando se realiza la misma tarea en repetidas ocasiones, por lo que si un gran grupo de alertas son falsos positivos entonces puede ser difícil para el analista establecer prioridades y ser acertado.

Los sistemas de detección de amenazas producen peta bytes de logs que necesitan ser procesados en tiempo real, por lo que se requiere una gran capacidad de procesamiento computacional para que puedan ser vistos por los analistas. El desarrollo de visibilidad, agilidad y velocidad, demanda una evolución en las capacidades analíticas de los SIEM [11].

**Requisitos de los Next-Gen SIEM**

Varios han sido los estudios y análisis que se han desarrollado en aras de determinar las funciones óptimas de los SIEM de nueva generación, los requisitos más recurrentes son los siguientes:

- Arquitectura de big data bien verificada:
  Para facilitar la efectividad en la capacidad de administración y la usabilidad, el SIEM moderno debe aumentar el volumen y la velocidad con una arquitectura de big data [12], [13].
  Se debe proporcionar un acceso preciso y rápido a los datos a través de búsquedas centralizadas y de alto rendimiento en datos estructurados y no estructurados, además debe permitir la indexación a gran escala y el almacenamiento de datos forenses durante meses o incluso años [1].
- Precio fijo:
  Los SIEM heredados generalmente tienen un precio por datos (EPS o GB) que obligan a los analistas de seguridad a descartar datos importantes relevantes para la seguridad y, por lo tanto, comprometer su capacidad de detección de amenazas. Las soluciones de análisis de seguridad funcionan mejor con cantidades cada vez mayores de datos y, por lo tanto, su precio no debe penalizar al cliente por el volumen de los mismos. En cambio, un SIEM de

próxima generación debería eliminar la imprevisibilidad de la ecuación al proporcionar un modelo de precios que se base en otras métricas que estén mejor alineadas con el negocio. Una métrica más adecuada a emplear sería el número de usuarios, ya que, aunque refleja con precisión el riesgo para la organización y la complejidad de las amenazas, logra que la solución de seguridad sea independiente de la cantidad de información necesaria para un rendimiento óptimo [12], [13].

- Contexto enriquecido de usuario y activos:
  El propósito de un SIEM es transformar una multitud de datos de seguridad dispares recopilados en información útil. Los SIEM heredados no pueden "conectar todos los puntos" al procesar la gran cantidad de datos operativos y de seguridad generados por la empresa moderna. Un SIEM de nueva generación debe usar la ciencia de datos para proporcionar contexto a esta información al enriquecer y aclarar detalles que se descubren, asignan y presentan automáticamente con sus objetos asociados [12], [13].
  Esto se logrará utilizando modelos estadísticos y aprendizaje automático para identificar más profundamente las relaciones entre el comportamiento de los datos y los elementos, y luego representar toda la información en contexto [1]. Lo anterior incluye el contexto sobre el usuario, el activo, la dirección IP, la ubicación geográfica, la inteligencia de amenazas, los resultados del análisis de vulnerabilidades, etc. Entonces, si se activa una alerta, la información del contexto se puede usar para aumentar automáticamente la prioridad de la misma, y también rápidamente comprender su gravedad según el actor, el activo en el que se identificó la amenaza y el tipo de datos en riesgo [13].
  A medida que un SIEM pueda contextualizar la información, aumentará la precisión de las reglas de detección, proporcionando a los analistas de seguridad de la información el contexto que necesitan para realizar investigaciones útiles.
  En resumen, el aprendizaje automático puede ayudar a agregar sentido a los datos disponibles, lo que aumenta las probabilidades de repeler ataques y prevenir infracciones [12].
- Comprensión del comportamiento normal:
  Para identificar con precisión las amenazas, un SIEM efectivo debe comprender el comportamiento "normal" de los usuarios y otras entidades en la red de la organización. El término de la industria para esta capacidad es Análisis de Comportamiento de Entidades y Usuarios (User and Entity Behavior Analytics o UEBA). Un SIEM moderno utiliza esta funcionalidad para identificar amenazas desconocidas y amenazas internas. El sistema detecta fácilmente las mismas al comprender cómo se comportan normalmente las máquinas y los humanos; luego encuentra actividad riesgosa y anómala que se desvía de esa línea de base [1], [12], [13].
  La línea de base conductual ocurre con tres elementos fundamentales de la ciencia de datos:
  - ✓ Aprendizaje automático
  - ✓ Análisis estadístico
  - ✓ Modelado conductual
- Gestión dinámica de la seguridad:
  Crear reglas de correlación es complicado y lleva mucho tiempo. Con ciber-ataques avanzados y dinámicos, también es un proceso constante a realizar en los SIEM heredados. Incluso con profesionales capacitados dedicados a administrar el SIEM, es imposible mantenerse al día con las amenazas que cambian a gran velocidad [12], [13].
  Una plataforma SIEM de próxima generación debe proporcionar contenido pre-empaquetado con la solución, pero también dinámico para adaptarse a las realidades de las ciber-amenazas actuales. El contenido de análisis de seguridad clasificado por el caso de uso y el tipo de amenaza, facilita a las empresas personalizar fácilmente su implementación para satisfacer sus necesidades únicas. Como beneficio adicional, emplear una comunidad sólida, típicamente en forma de intercambio de amenazas, ayuda con la necesidad de compartir contenido dinámico e información para mantenerse a la vanguardia de las amenazas en rápida evolución [12], [13].
- Habilitación de respuesta rápida a incidentes:
  Identificar las amenazas solo es parte del trabajo, responder rápidamente a las mismas es aún más crítico. Las plataformas de gestión de seguridad deben proporcionar capacidades automatizadas de respuesta a incidentes. Cada alerta identificada debe tener un libro de acciones recomendadas para los analistas forenses y los respondedores de incidentes.
  Este libro en un SIEM de próxima generación debe basarse en las mejores prácticas de la industria e incluir la capacidad de integrarse a través de API con soluciones de terceros, como herramientas de seguridad de red, dispositivos de protección de punto final, soluciones de escaneo, automatización de orquestación de seguridad (SOAR) y soluciones de inteligencia de amenazas. [1].

Las características de los SIEM de próxima generación pueden agruparse en una lista no exhaustiva, sin embargo, se han representado las más abarcadoras definidas hasta el momento. En general todas están diseñadas a la adaptación de los nuevos conceptos que engloban el Internet de las cosas (IoT) y el big data en la sociedad digital actual.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.1 , Enero-Abril, 2021, p.47-53 ISSN 1729-3804

## 4. AVANCES EN EL EMPLEO DE PLATAFORMAS DE NUEVA GENERACION EN CUBA

Actualmente existen diversos fabricantes que están liderando el desarrollo de SIEM de próxima generación, brindando soluciones robustas y de gran aceptación. Cada año la consultora Gartner realiza un análisis de estas tecnologías, ofreciendo una amplia valoración de sus funcionalidades y servicios. En la siguiente figura se pueden observar las soluciones más destacadas en el año 2018.


Figura. 1: Los SIEM líderes del 2018.

La mayoría de estas plataformas resuelven casi todos los problemas de seguridad planteados en este artículo, sin embargo todas requieren pago por licenciamiento y casi ninguna es de código abierto, como lo estipulan las regulaciones de Ciber-seguridad vigentes en el país. Al no existir una alternativas de libre costo en este tipo de tecnologías y que cumpla con todas las funcionalidades de un SIEM, diferentes empresas e investigadores de todo el mundo han desarrollado proyectos en aras de satisfacer sus necesidades con el menor costo posible.

En el caso de Cuba, una de las primeras empresas en moverse en este sentido fue la Empresa de Tecnologías de la Información para la Defensa, XETID.

El trabajo ha sido enfocado a la creación de un Centro de Inteligencia de Amenazas que base su funcionamiento en mecanismos de big data e inteligencia artificial (AI) y que en un futuro se integren con la plataforma SIEM OSSIM. El diseño general del proyecto contempla el trabajo integrado de herramientas como Suricata, Cuckoo Sandbox, Elastick, entre otras.

### Suricata

Suricata es un motor de detección de amenazas de red gratuito, de código abierto, maduro, rápido y robusto [14]. El motor Suricata es capaz de detección de intrusos en tiempo real (IDS), prevención de intrusos en línea (IPS), monitoreo de seguridad de red (NSM) y procesamiento pcap fuera de línea.
Suricata inspecciona el tráfico de la red utilizando un lenguaje potente y extenso de firma y reglas, y tiene un poderoso soporte de secuencias de comandos Lua para la detección de amenazas complejas [14].

### Cuckoo Sandbox

Cuckoo Sandbox es un software gratuito que automatiza la tarea de analizar cualquier archivo malicioso en Windows, MacOS, Linux y Android [15]. Es un sistema de análisis de malware automatizado avanzado, extremadamente modular y 100% de código abierto con infinitas oportunidades de aplicación [15].

### Elasticsearch

Elasticsearch es un motor de búsqueda y análisis RESTful distribuido, que almacena de manera centralizada sus datos para que pueda buscar, indexar y analizar datos de todas las formas y tamaños [16]. Es una nueva base de datos creada para manejar grandes cantidades de volumen de datos con una disponibilidad muy alta y para distribuirse en varias máquinas con el objetivo de ser tolerante a fallas y escalable, todo mientras mantiene una API simple pero poderosa que permite que aplicaciones desde cualquier lenguaje accedan a la base de datos [17].

### Resultados Obtenidos

Las demandas de un SIEM de próxima generación son ambiciosas, y aunque esta plataforma aun no cumple con todas ellas, ya es parte del Centro de Operaciones de Seguridad de la XETID. Su capacidad de detección de amenazas y análisis de malware han sido cruciales en la detección y prevención de incidentes en plataformas como la AC XETID (autoridad certificadora de la entidad), la plataforma EnZona (plataforma de comercio electrónico) y varias tiendas virtuales hospedadas en la entidad.

## 5. CONCLUSIONES

El surgimiento y desarrollo de la era digital ha traído consigo varios retos de ciber-seguridad para los cuales los Sistemas de Gestión de Información y Eventos de Seguridad que se emplean hoy en día no son suficientes. Es por ello que fue necesaria la concepción de un nuevo enfoque para los SIEM. La próxima generación de SIEM aumenta las capacidades tradicionales con tecnologías emergentes y ágiles como el análisis basado en la nube; orquestación de seguridad, automatización y respuesta [SOAR]; y análisis de comportamiento de usuarios y entidades [UEBA]; aprendizaje automático e inteligencia artificial. En Cuba se están dando los primeros pasos en aras de alcanzar el estado de seguridad requerido justo antes de que los volúmenes de datos sean los que lo exijan. Y aunque las redes nunca serán seguras, el empleo de estas tecnologías al menos las hace más fiables.

## RECONOCIMIENTOS

La autora desea agradecer al Ing. José Luis Chamizo Echevarría por su aporte invaluable para el desarrollo de esta investigación y a todos los que de una forma u otra han colaborado en la realización de la misma.

## REFERENCIAS

[1] B. Filkins, «An Evaluator´s Guide to NextGen SIEM», SANS Institute Information Security Reading Room, 2018.
[2] S. Dorigo, «Security Information and Event Management», Tesis de maestría, Radboud University Nijmegen, Nimega, 2012.
[3] «Security Information and Event Management Market», https://www.gartner.com/reviews/market/security-information-event-management, 2019. (accedido dic 11, 2019).
[4] P. Ribera-Vargas, «Sociedad digital y ciudadanía: un nuevo marco de análisis», Tecnologías digitales para transformar la sociedad, pp.145-153, España, 2018.

[5] J. Martín Carretero, C. Suero García, A. Suso Araico y J. Torres Mason, «Sociedad digital en España 2018», Fundación Telefónica, Madrid, 2019.
[6] M. Di Mauro y C. Di Sarno, «Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection», Journal of Information Security and Applications, Vol. 38, pp. 85–95, Aversa, Italy, 2018.
[7] L. Wang, R. Jones, «Big Data Analytics for Network Intrusion Detection: A Survey», International Journal of Networks and Communications 2017, Vol.7, No.1, pp. 24-31, Vicksburg, USA, 2017.
[8] O. Lindström, «Next Generation Security Operations Center», Bachelor's Thesis, Metropolia University of Applied Sciences, Finlandia, 2018.
[9] K. Al Jallad, M. Aljnidi, y M. S. Desouki, «Big data analysis and distributed deep learning for next-generation intrusion detection system optimization». Journal of Big Data, Vol.6 No.88, 2019.
[10] A. AwangLah, R. Akmam, y M. Hadri, «Proposed Framework for Network Lateral Movement Detection Based On User Risk Scoring in SIEM», 2018 2nd International Conference on Telematics and Future Generation Networks (TAFGEN), pp. 149-154, Kuching, 2018.
[11] R. Andrade y R. Torres, «Enhancing intelligence SOC with big data tools», 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1076-1080, Vancouver, BC, 2018.
[12] O. Cassetto, «10 Must-have Features to be a Modern SIEM», Exabeam, Inc., https://www.exabeam.com/siem/next-gen-siem/, 2019. (accedido ene 12, 2020).
[13] FireEye Cyber Defense Summit, «FireEye Combines Next-Generation SIEM With Advanced Orchestration and Cloud Security in HelixSecurity Operations Platform», Washinton, 2018.
[14] «Suricata», https://suricata-ids.org/, 2019. (accedido ene 10, 2020).
[15] «Cuckoo Sandbox - Automated Malware Analysis», https://cuckoosandbox.org/, 2019. (accedido feb 01, 2020).
[16] «Elasticsearch features list Elastic», https://www.elastic.co/es/products/elasticsearch/service, 2019. (accedido ene 12, 2020).
[17] M. Sai Divya, y S. Kumar Goyal, «ElasticSearch An advanced and quick search technique to handle voluminous data», COMPUSOFT, An international journal of advanced computer technology, Vol. 2, Issue. 6, pp. 171-175, 2013.

## SOBRE LA AUTORA

Lesly Núñez Jarrosay, A la edad de 15 años ingresó en la Fuerzas Armadas Revolucionarias de Cuba, donde en el año 2013 obtendría el título de Ingeniería en Telecomunicaciones y Electrónica otorgado por la Universidad Tecnológica de La Habana. Desde su graduación se dedicó al mundo de la Seguridad Informática en la Empresa XETID, principalmente dedicándose al mundo de los SIEM. En el año 2016 pasó el curso de Certificación de Alienvault USM y desde entonces ha colaborado en el diseño de la gestión de seguridad en diversos ministerios y entidades bancarias del país. **ORCID**: 0000-0001-7169-0019. **Categoría científica**: Ingeniera. **Organizaciones**: UIC

## CONFLICTO DE INTERESES

La autora declara que no existen conflictos de intereses.

## CONTRIBUCIONES DE LOS AUTORES

La autora realizó todo el desarrollo de la investigación, revisión de la literatura, confección del artículo y la revisión de las versiones para la publicación final.