BOLETIN CIENTÍFICO
IDEAS Y VOCES

# Utilización de AI en el monitoreo realizado por un (SOC): procesos formativos y de capacitación del personal técnico

***Use of AI in monitoring by a (SOC): training and education processes for technical personnel***

**Autor:**

Paul Canchignia Casco https://orcid.org/0009-0000-5552-1979

Jeovanny Benavides Bailón https://orcid.org/0000-0002-7606-2131

Institución y País

[1] *Pontificia Universidad Católica del Ecuador, Ecuador* pcanchignia0312@pucesm.edu.ec

[2] *Pontificia Universidad Católica del Ecuador, Ecuador* jbenavides@pucesm.edu.ec

**Recepción:** 05 de septiembre de 2024

**Aceptación:** 08 de octubre de 2024

**Publicación:** 05 de diciembre de 2024

**Citación/como citar este artículo:** Canchignia, P. y Benavides, J. (2024). Utilización de AI en el monitoreo realizado por un (SOC): procesos formativos y de capacitación del personal técnico. Ideas y Voces, 4(3), Pág. 275-295.

**Resumen**

En la actualidad resulta pertinente analizar el rol que cumple la utilización de la Inteligencia Artificial (AI) en los procesos de formación y monitoreo en un Centro de Operaciones de Seguridad (SOC). Se propicia la mejora de las capacidades de detección, respuesta y prevención de amenazas, de una organización unificando y coordinando todas las tecnologías y operaciones de ciberseguridad. El presente estudio tiene como propósito analizar el proceso formativo, académico y de instrucción que reciben los técnicos en materia de tecnologías innovadoras para afianzar la ciberseguridad en mención. Con un enfoque metodológico cuantitativo se permitió realizar la medición objetiva con generalización de resultados al permitir tener eficiencia en la recolección de datos mediante encuestas a 37 técnicos capacitados en procesos de formación con la utilización de herramientas de AI. Para ello, se propone un análisis comparativo de la capacidad analítica con la que cuenta el personal técnico de Nivel 1, una vez que ha sido capacitado y entrenado en el uso de herramientas de AI; explorando estrategias educativas mediante prácticas en turnos operativos. El resultado de este trabajo es comprobar el aporte de la AI en la capacidad analítica de los técnicos Nivel 1 del SOC.

**Palabras clave:** Competencias innovadoras; Seguridad; amenazas cibernéticas; Inteligencia Artificial; procesos de formación.

**Abstract**

It is currently relevant to analyze the role that the use of Artificial Intelligence (AI) plays in the training and monitoring processes in a Security Operations Center (SOC). It promotes the improvement of the detection, response and prevention capabilities of an organization by unifying and coordinating all cybersecurity technologies and operations. The present study aims to analyze the training, academic and instructional process that technicians receive in the field of innovative technologies to strengthen cybersecurity. With a quantitative methodological approach, it was possible to carry out objective measurement with generalization of results by allowing efficiency in data collection through surveys to 37 technicians trained in training processes using an AI tool (Darktrace). To do this, a comparative analysis of the analytical capacity of Level 1 technical staff, once they have been trained and trained in the use of AI tools, is proposed; exploring educational strategies through shift-based practices. The result of this work is to test the contribution of AI in the analytical capacity of SOC Level 1 technicians.

**Keywords**

Innovative skills; Security; Cyber threats; Artificial intelligence; Training processes.

## Introducción

En este sentido, se asumen que el profesional de la tecnología en ciberseguridad debe estar en capacidad de entender los modelos de bases de datos para determinar en dónde y cómo se deben implementar las seguridades que mitiguen las ciber amenazas. Además, según Caracciolo (2022), debe realizar informes técnicos relacionados con incidentes de ciberseguridad usando un lenguaje técnico apropiado y siguiendo una estructura adecuada del mismo. También se espera que sea capaz de entender su rol dentro de la sociedad, desde el punto de vista ético, para aplicar los conocimientos adquiridos en esta temática.

A criterio de Portella (2022), la Inteligencia Artificial está entrando de forma acelerada en el dominio de la ciberseguridad, de la mano de los grandes actores tecnológicos que realizan grandes inversiones impulsadas por planes estratégicos. Las agencias de seguridad y estándares analizan y clasifican la aplicación de la IA a la seguridad.

En los últimos años la ciberseguridad demanda de forma creciente la introducción de recursos tecnológicos y organizativos en un escenario de riesgo creciente y exigencia normativa. Según Krishnappa (2023), la relevancia de Microsoft en el panorama de la ciberseguridad es inmensa. Sus productos están en prácticamente toda la superficie de exposición.

Para Marcel (2023), las mayores cibercrisis a nivel planetario se han originado en torno a vulnerabilidades de los productos de este gigante tecnológico. Tanto la tendencia geopolítica como la industria y la dinámica de la ciberseguridad están introduciendo la Inteligencia Artificial con celeridad en el escenario. La complejidad de esta tecnología, la carencia de especialistas, su rápida evolución, el coste de las soluciones, hacen inviable una aproximación interna o en solitario.

Según Mérida (2019), la mayoría de los incidentes de seguridad de los últimos 5 años, no sucedieron por la astucia y conocimiento de personas mal intencionadas que explotaron fallas en los servidores, sino por descuidos de los empleados de las propias organizaciones. Pensar y diagramar la ciberseguridad de una organización no se trata solo de tecnología, se trata de procesos y personas también. Incorporar tecnología claramente es importante y ayuda, pero es mucho más importante “entrenar” a equipos de trabajo para que sus procesos sean seguros desde el diseño (no solo concienciar). Para Navarro y Guerrero (2022), la tecnología en materia de monitoreo y defensa ha mostrado un

entendimiento de la necesidad propia de la industria y se ha adaptado a la misma logrando ingresar al mercado con mucha facilidad.

Desde la perspectiva de Sigala (2023), en la perspectiva actual de la constante evolución de las amenazas cibernéticas, el SOC desempeña un papel fundamental en las fases de preparación, detección, análisis, contención, erradicación y recuperación ante la explotación de vulnerabilidades en tiempo real. Sin embargo, el volumen creciente y la complejidad de los datos generados por las redes y sistemas de información han hecho que la tarea de monitorear estas amenazas por parte del personal técnico del Nivel 1 de un SOC, sea cada vez más desafiante dado que los mismos como primera línea de defensa en un SOC enfrentan una creciente presión para identificar y responder rápidamente a este tipo de amenazas.

Sontan y Samuel (2024) explican que, en respuesta a esta creciente demanda, la integración de la AI en las operaciones de monitoreo del SOC ha surgido como una herramienta poderosa para mejorar la eficiencia y la precisión del monitoreo, desarrollando nuevas destrezas mediante la capacitación del personal técnico de Nivel 1 en esta tecnología. En este artículo, exploramos cómo la utilización de la AI puede beneficiar el proceso de monitoreo en un SOC, con un enfoque particular en la capacitación de los técnicos de nivel 1.

Según Velasco (2023), la estrecha interacción entre la AI y la ciberseguridad emerge como un aspecto de suma importancia, destacando el papel fundamental del aprendizaje automático en la resolución de desafíos en este campo. Recientemente, han surgido iniciativas como "IA y ciberseguridad para adolescentes", cuyo propósito radica en la integración de la AI y el aprendizaje automático en el plan de estudios de la educación secundaria, abordando de manera simultánea aspectos éticos y prejuicios inherentes, mediante el empleo de herramientas como NetsBlox, un entorno de programación basado en bloques fácil de usar. Adicionalmente, se comparten las experiencias de talleres piloto con docentes de ciberseguridad, quienes han manifestado comentarios positivos, a pesar de identificar algunos desafíos en su implementación en el aula (Grover 2023).

Por otra parte, frente a la creciente demanda de recursos y pericia en ciberseguridad, resulta alentador enfocarse en el seguimiento y detección de amenazas en el SOC, utilizando escenarios de ataque y defensa en entornos configurados. Mientras que los escenarios de defensa se concentran en la operación de un SOC, los escenarios de ataque simulan la actividad de un SOC configurado en sistemas de información vulnerables. Los resultados, en su mayoría, ponen de manifiesto una falta de integración entre la literatura

sobre SOC funcional y los escenarios de ataque y defensa, así como la carencia de directrices prácticas para su implementación en entornos educativos. Como parte de la solución, se propone una estructura teórica y una topología de un entorno para la formación aplicada en ciberseguridad, que utiliza sistemas de información vulnerables como objetivos de ataque y un SOC para la detección y respuesta a dichos ataques (Gerontakis 2022).

La ciberseguridad se ha convertido en un pilar fundamental para proteger los activos digitales de individuos, organizaciones y gobiernos contra las crecientes amenazas cibernéticas. La evolución de tecnologías como la Inteligencia Artificial (IA) ha introducido nuevas posibilidades y desafíos en el campo de la seguridad informática. La integración de la IA en la ciberseguridad promete revolucionar la forma en que detectamos, respondemos y nos defendemos contra las amenazas en línea. Desde la detección avanzada de amenazas hasta la automatización de respuestas a incidentes, la IA ofrece un conjunto diverso de herramientas y capacidades que pueden fortalecer nuestras defensas cibernéticas (Sontan & Samuel 2024). En este contexto, es fundamental comprender cómo la IA ayuda a los analistas de seguridad a detectar anomalías, reducir costos y fortalecer las defensas cibernéticas. Además, la adopción de tecnologías de IA en la protección de datos se vuelve crucial debido al aumento de las amenazas, la necesidad de cumplir con regulaciones de privacidad y la importancia de mantener la eficiencia operativa en un entorno digital en constante evolución (Krishnappa 2023).

Así como Mosquera (2019), Grover (2020) partió del enfoque en diseñar y buscar comentarios de profesores de ciberseguridad y AI, así como capacitarlos en estos materiales para que luego pudieran integrarlos en sus planes de estudio. Grover señala que existe una necesidad de materiales de apoyo de alta calidad, además de las actividades lectivas en sí, para abordar las inquietudes de los docentes sobre la enseñanza de estos temas nuevos para ellos. Sus censos señalan que últimamente las materias en el currículum del American College Test (ACT) solapan adecuadamente a la AI con la Ciberseguridad, cubriendo programas no solo desafiantes sino innovativos (de acuerdo a la opinión de 12 profesores durante 2 distintos talleres en escuelas secundarias).

Krishnappa (2018) tiene una perspectiva similar a Mosquera (2020), pues argumenta que la AI mejora la seguridad a pesar de presentar riesgos, pues destaca la necesidad de colaboraciones éticas entre humanos y AI, especialmente en contextos de seguridad. Aunque la AI cuenta hoy en día con una inteligencia y velocidad superiores, requiere la intervención humana para funcionar eficazmente. Las empresas deben invertir en la

formación de expertos en AI para garantizar la seguridad del producto. Al integrar la AI con el intelecto humano, las organizaciones pueden fortalecer las defensas contra los hackers. En general, la AI promete revolucionar las medidas de seguridad, ofreciendo soluciones avanzadas para combatir las amenazas cibernéticas en un futuro cercano.

**Metodología**

El enfoque central de esta investigación es explorar y determinar si la AI puede mejorar la capacidad de análisis de los técnicos de nivel 1 de un SOC, mediante la capacitación basada en esta herramienta en la detección y clasificación de amenazas, la automatización de tareas repetitivas, el soporte en la toma de decisiones y la mejora continua mediante el aprendizaje automático.

Se empleó la investigación cuantitativa para realizar la medición objetiva con generalización de resultados, permitiéndonos tener eficiencia en la recolección de datos mediante encuestas y experimentos controlados. En este caso, el objetivo principal es evaluar el impacto de la AI en el monitoreo del SOC y su efecto en la capacitación y desempeño de los técnicos de Nivel 1. Para alcanzar este objetivo, se ha considerado pertinente seguir una metodología cuantitativa (Ñaupaz, 2014). Una encuesta como técnica será efectiva para recopilar datos cuantitativos sobre la percepción, el conocimiento, así como las habilidades del personal técnico de Nivel 1 en relación con la utilización de AI en el monitoreo del SOC. Se diseñará una encuesta estructurada que contenga preguntas específicas relacionadas con el uso de AI y sus beneficios percibidos. Un cuestionario estructurado sería el instrumento adecuado para llevar a cabo la encuesta, mismo que estará diseñado de manera clara y precisa para recopilar datos relevantes y objetivos.

**Procesamiento y análisis estadístico**

**Resultados**

Entre las variables clave se considera la competencia de los técnicos de Nivel 1 antes y después de la implementación de la AI, para lo cual se procede a encuestar a 37 analistas Nivel 1 de un SOC. Se utilizan técnicas estadísticas para analizar los datos recopilados y determinar si hay diferencias significativas entre el grupo experimental y el grupo de control en términos de eficiencia del monitoreo y competencia de los técnicos de nivel 1. Los resultados se encuentran basados en un estudio previo de Mosquera (2021), quien se proyectó en el estudio de la interconexión de la AI con la Ciberseguridad, así como con la utilidad de asimilar el conocimiento de estas dos especialidades.

En el presente estudio a través de la investigación y evaluación de la utilización de AI en las operaciones de un SOC, se busca identificar las ventajas y limitaciones de esta tecnología en la capacitación del personal técnico de Nivel 1. Se analizarán detalladamente los resultados obtenidos, incluyendo la precisión en la detección de amenazas, la reducción del tiempo de respuesta ante incidentes y la mejora en la eficiencia operativa del SOC. Además, se explorarán las implicaciones prácticas y estratégicas de la implementación de la AI en el contexto de la formación del personal de Nivel 1, así como las posibles áreas de mejora y recomendaciones para futuras investigaciones y desarrollos en este campo en constante evolución. Esta discusión crítica proporcionará una base sólida para comprender el impacto y el potencial de la AI en el fortalecimiento de la capacidad de análisis a nivel operativo, destacando su papel como una herramienta fundamental en la defensa contra las amenazas digitales emergente.

Adicional, es importante determinar la familiaridad con el uso de tecnologías de AI en el entorno de seguridad cibernética. Este dato preliminar fue fundamental para contextualizar los resultados posteriores y comprender mejor las características de la muestra.

Posteriormente, se examinó el nivel de conocimiento y experiencia práctica del personal de Nivel 1 en lo que respecta al uso de AI en el monitoreo del SOC. Esto implicó evaluar la comprensión de conceptos clave relacionados con la inteligencia artificial, así como la experiencia previa con herramientas específicas de AI utilizadas en la detección y respuesta a amenazas cibernéticas. El análisis de estos datos reveló insights importantes sobre el grado de familiaridad y competencia del personal en la integración de tecnologías de AI en sus actividades diarias de monitoreo y análisis de seguridad.

El estudio sobre la vinculación entre la AI y la seguridad cibernética en Ecuador destaca la necesidad urgente de que el Estado establezca medidas para proteger a los ciudadanos y la infraestructura crítica de las crecientes amenazas en línea, con el fin de prevenir y reaccionar ante ataques informáticos cada vez más sofisticados, pero manteniendo la participación humana en la toma de decisiones. Además, se enfatiza la importancia de concienciar, capacitar y difundir buenas prácticas de seguridad informática, pues los ataques cibernéticos suelen estar dirigidos a los eslabones débiles de la cadena de seguridad, es decir, usuarios desprovistos de sistemas de protección adecuados y robustos (Mosquera, 2021).

Como se explicó en el apartado anterior, el presente estudio ha tenido como propósito analizar el proceso formativo, académico y de instrucción que reciben los técnicos en materia de tecnologías innovadoras para afianzar la ciberseguridad en mención. En base a ello se describen los siguientes resultados.

**Tabla 1**

*Interés por la interconexión de la AI con Ciberseguridad*

| Variables | Técnicos N1 | Porcentaje (%) |
|---|---|---|

| | | |
|---|---|---|
| Totalmente de acuerdo | 16 | 43 |
| De acuerdo | 10 | 27 |
| En desacuerdo | 2 | 5 |
| Totalmente en desacuerdo | 4 | 11 |
| Ni de acuerdo ni en desacuerdo | 5 | 14 |
| Total | 37 | 100 |

Fuente: Mosquera (2021)

En la Tabla 1 muestra que una mayoría significativa, el 70% de los encuestados (43% totalmente de acuerdo + 27% de acuerdo), está a favor de la interconexión entre la Inteligencia Artificial y la Ciberseguridad, mientras que solo un pequeño porcentaje, el 16% (5% en desacuerdo + 11% totalmente en desacuerdo), se opone a esta idea.

En resumen, la aplicación de la AI con Ciberseguridad denota interés en los técnicos de Nivel 1 ya que es parte de la evolución de la tecnología y además trae consigo mayores ventajas para el monitoreo de las alertas de ciberseguridad.

Ahora, así como Mosquera, Grover partió del enfoque en diseñar y buscar comentarios de profesores de ciberseguridad y AI, así como capacitarlos en estos materiales para que luego pudieran integrarlos en sus planes de estudio. Grover señala que existe una necesidad de materiales de apoyo de alta calidad, además de las actividades lectivas en sí, para abordar las inquietudes de los docentes sobre la enseñanza de estos temas nuevos para ellos. Sus censos señalan que últimamente las materias en el currículum del American College Test (ACT) solapan adecuadamente a la AI con la Ciberseguridad, cubriendo programas no solo desafiantes sino innovativos (de acuerdo a la opinión de 12 profesores durante 2 distintos talleres en escuelas secundarias). Por tal razón, la opinión de replicar los contenidos de las asignaturas en posteriores cursos es de hasta el 100% en algunos casos.

**Tabla 2**

*Utilidad por tener conocimiento acerca de la AI y Seguridad Cibernética*

| Variables | Técnicos N1 | Porcentaje (%) |
|---|---|---|
| Totalmente de acuerdo | 20 | 54 |
| De acuerdo | 10 | 27 |
| En desacuerdo | 1 | 3 |
| Ni de acuerdo ni en desacuerdo | 6 | 16 |
| Total | 37 | 100 |

Fuente: Mosquera (2021)

En la **Tabla 2** muestra que una amplia mayoría, el 81% de los encuestados (54% totalmente de acuerdo + 27% de acuerdo), considera útil poseer conocimientos sobre AI y Seguridad Cibernética.Solo una minoría muy pequeña, el 3% de los encuestados está en desacuerdo con esta idea.

En resumen, el tener conocimientos acerca de la AI y de seguridad cibernética muestra un interés en los técnicos de Nivel 1, esto indica un reconocimiento generalizado entre los encuestados de laimportancia y relevancia de estas áreas en el contexto actual de la tecnología y la seguridad digital.La percepción compartida de que el conocimiento en AI y Seguridad Cibernética es valioso sugiere una conciencia creciente sobre la necesidad de estar preparado y capacitado para enfrentar los desafíos emergentes en el ámbito de la seguridad informática, así como aprovechar las oportunidades que ofrecen las tecnologías avanzadas como la AI para mejorar la protección de sistemas y datos.

Krishnappa tiene una perspectiva similar a Mosquera, pues argumenta que la AI mejora la seguridad a pesar de presentar riesgos, pues destaca la necesidad de colaboraciones éticas entre humanos y AI, especialmente en contextos de seguridad. Aunque la AI cuenta hoy en día con una inteligencia y velocidad superiores, requiere la intervención humana para funcionar eficazmente. Las empresas deben invertir en la formación de expertos en AI para garantizar la seguridad del producto. Al integrar la AI con el

intelecto humano, las organizaciones pueden fortalecer las defensas contra los hackers. En general, la AI promete revolucionar las medidas de seguridad, ofreciendo soluciones avanzadas para combatir las amenazas cibernéticas en un futuro cercano.

**Tabla 3**

*Beneficio de la utilización de herramientas basadas en AI en Ciberseguridad*

| Variables | Técnicos N1 | Porcentaje (%) |
|---|---|---|
| Totalmente de acuerdo | 30 | 81 |
| De acuerdo | 7 | 19 |
| Total | 37 | 100 |

Fuente: Portela (2022)

En la **Tabla 3** muestra que una amplia mayoría, el 100% de los encuestados (81% totalmente de acuerdo + 19% de acuerdo), considera útil poseer conocimientos sobre AI y Seguridad Cibernética.En resumen, el uso de herramientas basadas en AI en el ámbito de la ciberseguridad indica que lostécnicos N1 mejoran notablemente el análisis de primer nivel debido a los beneficios que estas herramientas pueden aportar en la detección, prevención y respuesta a amenazas cibernéticas.

Estos hallazgos coinciden con la visión de Santiago Portela sobre el papel fundamental que desempeña la Inteligencia Artificial en la ciberseguridad. Portela destaca cómo la IA está transformando tanto la defensa como las amenazas en el campo de la ciberseguridad, siendo un elemento clave en la protección de sistemas y datos en un entorno cada vez más digital y conectado (Portela 2022). La creciente conciencia sobre la importancia de la IA y la ciberseguridad entre los técnicos de Nivel 1 refleja la relevancia y actualidad de estos temas en el ámbito tecnológico y de seguridad digital, tal como lo señala Portela en su investigación. Por otro lado, Victor Mendes en su obra "Marco Técnológico de un SOC de nueva generación" destaca la importancia de contar

con tecnologías avanzadas y personal altamente calificado para hacer frente a las amenazas cibernéticas en evolución y para mejorar la eficacia de los Centros de Operaciones de Seguridad (SOC).

**Tabla 4**

*Grado de explicabilidad y visibilidad que se tiene sobre la solución*

| Variables | Técnicos N1 | Porcentaje (%) |
|---|---|---|
| Totalmente de acuerdo | 20 | 54 |
| De acuerdo | 10 | 27 |
| Ni de acuerdo ni en desacuerdo | 7 | 19 |
| Total | 37 | 100 |

Fuente: Portela (2022)

En la **Tabla 4** muestra que una amplia mayoría, el 81% de los encuestados (54% totalmente de acuerdo + 27% de acuerdo), indicaron que se debe de tener un grado de visibilidad y explicabilidad[1]proporcionado por la solución. Sin embargo, la presencia de un grupo minoritario (19%) que no expresó una opinión clara señala la necesidad de una comunicación más clara y una mayor transparencia por parte de los proveedores de soluciones de IA en Ciberseguridad para garantizar una comprensión completa y una confianza adecuada por parte de todos los involucrados.

En resumen, el tener un grado de explicabilidad (aplica al empleo de AI) y visibilidad de la solución para el monitoreo por parte de los técnicos N1 ayuda a tener una comunicación clara y transparente acerca del funcionamiento de la herramienta mejorando así los conocimientos y la experiencia delN1 en la herramienta.

Estos hallazgos pueden ser complementarios a la investigación de Santiago Portela, quien destaca el papel fundamental que desempeña la IA en la ciberseguridad y cómo está transformando tanto la defensa como las amenazas en este campo. La necesidad

de visibilidad y explicabilidad en las soluciones de IA en ciberseguridad, como se refleja en la Tabla 4, puede estar relacionada con la importancia de comprender y confiar en las tecnologías avanzadas utilizadas para proteger sistemas y datos en un entorno digital cada vez más complejo y conectado. Por otro lado, Mendes hace énfasis en la interoperabilidad con tecnologías de seguridad emergentes, la importancia de la automatización en la seguridad, la necesidad de capacidades de análisis avanzadas y el uso de herramientas como SIEM, EDR, UEBA, TIP y SOAR. Ambos aspectos resaltan la importancia de la comunicación clara, la transparencia y la capacitación adecuada para enfrentar los desafíos en el ámbito de la seguridad informática en un entorno tecnológico en constante evolución. Finalmente, este resultado se alinea en la investigación de Tomas Navarro destacando la importancia de la explicabilidad en las soluciones de inteligencia artificial en ciberseguridad, como se menciona en el artículo. La transparencia y la capacidad de comprender cómo funciona una solución de IA son aspectos cruciales para mejorar el conocimiento y la experiencia de los técnicos N1 en el uso de la herramienta.

**Tabla 5**

*Utilización de herramientas de automatización*

| Variables | Técnicos N1 | Porcentaje (%) |
|---|---|---|
| Totalmente de acuerdo | 15 | 41 |
| De acuerdo | 10 | 27 |
| En desacuerdo | 5 | 14 |
| Ni de acuerdo ni en desacuerdo | 7 | 19 |
| Total | 37 | 100 |

Fuente: Portela (2022)

En la **Tabla 5 se** muestra una percepción mixta entre los técnicos N1, el 68% de los encuestados (41%totalmente de acuerdo + 27% de acuerdo), indicaron que el uso de

herramientas de automatizacióncomo SOAR ayuda a priorizar el análisis de Nivel 1. Sin embargo, la presencia de un grupo minoritario (14%) expresó que está en desacuerdo con esta idea. Además, el 19% de losencuestados que no expresaron una opinión clara destacan la necesidad de una mayor claridad y comprensión sobre los beneficios y posibles desafíos asociados con el uso de herramientas de automatización en este ámbito.

En resumen, el contar con una herramienta de automatización para el monitoreo por parte de los técnicos N1 puede representar una mejora en la priorización de eventos de ciberseguridad que requieran un mayor tiempo de análisis.

Este hallazgo en contraste con Tomas Navarro refleja la importancia de una mayor claridad y comprensión sobre los beneficios y posibles desafíos asociados con el uso de herramientas de automatización en ciberseguridad. La presencia de un grupo minoritario que no está de acuerdo y otro grupo que no expresó una opinión clara resalta la necesidad de una comunicación más efectiva y una mejor formación sobre las ventajas de la automatización en este contexto, por otro lado, en relación con las herramientas de automatización en el obra de Méndez Fonseca, se destaca la importancia de la automatización para liberar a los analistas de seguridad de tareas repetitivas y permitirles enfocarse en la detección proactiva de amenazas y la colaboración con otras áreas de la organización.

**Discusión**

La interacción que existe entre la Inteligencia Artificial y la Ciberseguridad ha crecido de manera exponencial, debido a que actualmente en el mercado ya se han incorporado esta integración en los productos de protección basadas en el Aprendizaje de Máquina (Machine Learning o ML). Por otro lado, La AI también es un factor de mejorar en la

elaboración de malware que elude la protección proporcionada por las herramientas basadas en AI (Portela 2022).

Actualmente, el ML está siendo ampliamente utilizado al elaborar un modelo predictivo a partir de la utilización de métodos analíticos y de clasificación que aprende continuamente en los diferentes casos de uso a los que se encuentra expuesto. La forma común de crear el modelo es con el uso de Redes Neuronales, que simulan un conjunto de capas neuronales que se conectan entre sí, una forma avanzada del ML es el Deep Learning (Aprendizaje profundo o DL), el cual se caracteriza por tener un algoritmo de aprendizaje estructurado de tal manera que se modifica y evoluciona en base a la experiencia (Sigala 2023).

En base al antecedente antes mencionado, varios proveedores relevantes del mercado de la ciberseguridad están invirtiendo en la incorporación y desarrollo de la AI (Julio 2020), por ejemplo, los siguientes proveedores:

- Check Point: Se caracteriza por un servicio centralizado en Campaing Hunting, el cual se encarga de explorar todos los puntos de la red en busca de anomalías, mediante un aprendizaje continuo basado en ML.
- DarkTrace: Está enfocada a la prevención de intrusión en redes WAN, LAN y WIFI. Sus modelos de ML aprenden constantemente del comportamiento de la red sin la intervención humana, adaptándose al entorno del cliente y mejorando la capacidad de defensa.
- Fortinet: Incorpora DL supervisado en sus modelos de ML, de tal manera que se crean redes neuronales profundas para ofrecer un sistema dotado de autoaprendizaje que aprende de la red.

- IBM: Mediante ML brinda respuestas rápidas y predictivas en su correlacionador de eventos de Ciberseguridad Qradar
- Palo Alto: Usa la combinación de ML supervisado y no supervisado en el aprendizaje de sus modelos, el cual absorbe todo el comportamiento de la red a través de SIEM y traza una línea base de comportamiento ofreciendo una "seguridad continua".

Hoy en día, la intentar establecer una capa de seguridad a una empresa que maneje activos de TI se piensa de manera activa en la implementación de controles de acceso fortaleciendo reglas en firewalls, actualización de firmas de IPS o antivirus u otros controles en los dispositivos perimetrales de la red, si bien es cierto, estas medidas son efectivas, estas no son suficientes para mejorar establecer un nivel de madurez en la seguridad informática, por lo que, las empresas deben de estar en la capacidad de monitorear constantemente su infraestructura crítica y así detectar cualquier actividad anormal que se puede dar tanto internamente como externamente de la red (Julio 2020).

La implementación de un SOC (Security Operations Center) en respuesta a esta problemática requiere de una gran cantidad de tiempo en aspectos como: planeación, evaluación e implementación; la implementación de un SOC nace de la necesidad de gestionar y contener las amenazas que existen con el crecimiento del internet y dar respuesta oportuna y precisa ante estas amenazas.

El personal técnico capacitado (Analistas N1) está en la responsabilidad de contar con las herramientas adecuadas para realizar la revisión de registros (logs) de diferentes fuentes de información, por ejemplo: firewalls, IPS, antivirus, vulnerabilidades, actividad en la red, entre otros, dicha actividad debe ser centralizada mediante una herramienta SIEM, la

cual debe tener la capacidad de centralizar toda la actividad de la red proveniente de múltiples orígenes y dar un valor agregado sobre dichos eventos (Julio 2020). Y en este punto es donde entra la participación de las herramientas basadas en Inteligencia Artificial, las cuales brindan un amplio espectro o visibilidad de la red y todo el tráfico que se encuentra en ella, de tal manera, que el personal técnico tiene completa visibilidad de lo que está sucediendo en tiempo real.

La automatización juega un papel importante en la seguridad debido a los miles de alertas que recibe el SOC diariamente que sobrepasa la capacidad de análisis humana (Navarro, Guerrero 2022). En respuesta a esta problemática cada vez más grande nace la herramienta SOAR (Security Orchestration, Automation and Response) la cual permite a las organizaciones recopilar entradas monitoreadas por el SOC a través de las alertas del SIEM, donde se realiza el análisis, priorización y clasificación de incidentes de tal manera que las herramientas SOAR permite a una organización definir el análisis de incidentes y los procedimientos de respuesta en un formato de flujo de trabajo digital. Esta automatización impulsada por BIG DATA permite a los equipos tomar decisiones más rápidas y acertadas reduciendo la cantidad de falsos positivos en las alertas (Julio 2020).

A través de automatizaciones de acciones como bloquear direcciones IP, suspender cuentas de usuario o poner en cuarentena los dispositivos finales de los usuarios de una red, la herramienta SOAR puede reducir el tiempo de respuesta y por consiguiente reducir el daño potencial y las interrupciones que puedan provocar (Navarro, Guerrero 2022).

El SOC debe tener conocimientos y capacidad para manipular las diferentes herramientas que satisfacen con los siguientes aspectos:

- Monitoreo activo de la infraestructura con el objetivo de establecer una detección temprana de amenazas por lo que se pueden identificar, evaluar y corregir las diferentes vulnerabilidades presentes en la red (Marcel 2023).

- Controles de acceso, es decir, la implementación de whitelists y blacklists para permitir o restringir el tráfico desde y hacia la red (Marcel 2023).
- Detección y análisis de malware, es decir, tener la capacidad de detectar, identificar y desactivar algún tipo de programa considerado como malicioso (Marcel 2023).
- IDS/IPS, estar en la capacidad de detectar y bloquear cualquier tiempo de comportamiento anómalo dentro de la red (Marcel 2023).
- Gestión de incidentes, es decir, el uso de un SIEM en el monitoreo activo de los recursos de TI (Marcel 2023).

Además de tener con elementos tecnológicos para el monitoreo activo de la infraestructura de TI de una organización, se debe tener dentro de las filas de especialistas N1 personal con habilidades en la caza de amenazas, el cual corresponde al acto de encontrar formas, patrones y comportamientos anómalos que puedan indicar posibles escenarios de ataques o intrusiones (Julio, 2020).

Cada analista debe desarrollar habilidades competentes para realizar la cacería de amenazas que únicamente se desarrollan en base la experiencia y en el análisis de anomalías presentes en la red, el comprender los TTPs (Técnias, Tácticas y Procedimientos) empleados en base a los vectores de ataque que pueden ser usados por atacantes.

**Conclusiones**

El presente estudio tuvo como propósito analizar el proceso formativo, académico y de instrucción que reciben los técnicos en materia de tecnologías innovadoras para afianzar la ciberseguridad en mención.

En este contexto, el uso de algoritmos de Aprendizaje Automático está experimentando niveles significativos de desarrollo y desempeño en base a los datos disponibles. Algunos de estos algoritmos son capaces de aprender y ejecutar tareas sin requerir una programación explícita. Se han identificado numerosos casos de uso que van desde la organización de datos hasta la identificación de patrones relevantes dentro de conjuntos de datos específicos.

La implementación de la herramienta SOAR juega un papel crucial en la automatización parcial o total de una serie de actividades para que el personal de seguridad tenga más tiempo para buscar amenazas en lugar de responder a ellas.

La integración entre la AI y la ciberseguridad mejora las capacidades de operación de los técnicos de Nivel 1 pertenecientes al SOC, de tal manera que cualquier tipo de ataque puede ser detectado y mitigado antes de ocasionar daños a las organizaciones.

Los analistas técnicos de Nivel 1 del SOC debe contar con el conocimiento y capacidades de manejar diversas herramientas como DarkTrace, Qradar para el monitoreo activo de los activos críticos en la infraestructura de TI.

La educación continua en temas de soluciones de ciberseguridad basadas en AI juega un papel importante dentro del análisis realizado por los analistas de Nivel 1, tanto en el manejo de la herramienta como en la calidad del reporte enviado.

El SOC debe adoptar una postura proactiva frente a las amenazas, ya que este enfoque no puede automatizarse completamente. Por lo tanto, resulta crucial que los analistas técnicos de Nivel 1 aprovechen y enriquezcan su base de conocimientos a través de la experiencia diaria al correlacionar eventos.

**Referencias Bibliográficas**

Blanco, P. y Del Toro, J. (2022). Ciberseguridad y formación para no técnicos en el sector de la seguridad privada. Seguritecnia, 494, 104-105. https://www.seguritecnia.es/revistas/seg/494/104/index.html

Caracciolo, C. (2022). La evolución en ciberseguridad no es sólo tecnología. @ntena, 199, 2022, 37. https://www.telecos.zone/media/attachments/2023/09/26/revista-antena---n-199-mayo-2022_2.pdf

Georgios Gerontakis, Ioannis Voyiatzis, & Yannakopoulos, P. H. (2022). Security Operations Center in Education: Building an Educational Environment for Attack and Defense Scenarios. *PCI '22: Proceedings of the 26th Pan-Hellenic Conference on Informatics*, 27–31. Association for Computing Machinery. https://doi.org/10.1145/3575879.3575962

Grover, S., Broll, B., & Babb, D. (2023). Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. *In Proceedings of the 54th ACM Technical Symposium on Computer Science Education , 1*, 980–986. Association for Computing Machinery. https://doi.org/10.1145/3545945.3569750

Julio, M. F. V. (2020). *Marco Tecnológico de un SOC de nueva generación*. http://repository.unipiloto.edu.co/handle/20.500.12277/7937

Krishnappa, T. (2023). A review on artificial intelligence techniques in preventing cyber threats. *International Journal Of Engineering Applied Sciences And Technology*, *8*(1), 185-189. https://doi.org/10.33564/ijeast.2023.v08i01.029

Marcel, R. V. P. (2023). *Análisis de funcionalidad y utilidad de herramientas de seguridad instaladas en un Security Operation Center (SOC)*. http://repositorio.uisrael.edu.ec/handle/47000/3556

Mérida, J. (2019). Técnicas reunidas la ciberseguridad en una ingeniería en transformación. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 28(134). 164-165. https://revistasic.es/revista-sic-numero-134/

Mosquera, S. (2021). La vinculación entre la inteligencia artificial y la seguridad cibernética en el Ecuador. Notas sobre una interconexión necesaria. *Polo del Conocimiento*, *6*(2), 1154- 1173. https://polodelconocimiento.com/ojs/index.php/es/issue/view/77

Ñaupas, H. (2014). *Metodología de la investigación cuantitativa - cualitativa y redacción de la tesis* (4th ed.). Bogotá, Colombia Ediciones De La U. http://librodigital.sangregorio.edu.ec/librosusgp/B0028.pdf

Navarro, T. S., & Guerrero, A. G. (2022). El SOC "Autónomo": Inteligencia Artificial para la nueva ciberseguridad. Universidad de castilla La Mancha. *Seguridad de la información*, 19. https://revista.uclm.es/index.php/ruiderae/article/view/3088

Portela, S. (2022). Panorama de la inteligencia artificial en el dominio de la ciberseguridad. *RUIDERAe: Revista de Unidades de Información. (ISSN 2254-7177)*, *19*. Universidad de Castilla~La Mancha. https://revista.uclm.es/index.php/ruiderae/article/view/3082

Sigala, M. Q. (2023). Aplicaciones de la inteligencia artificial en contribución a la defensa nacional de chile. Una oportunidad para la integración de la defensa, la industria y la academia. *Política y Estrategia*, 141, 155-185. https://doi.org/10.26797/rpye.vi141.1044

Sontan, A., & Samuel, S. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal Of Advanced Research And Reviews*, *21*(2), 1720-1736. https://doi.org/10.30574/wjarr.2024.21.2.060

Velasco, J. (2022). Ser o no ser digital. Sin identidad no hay ciberseguridad. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 31(152), 107-148. https://revistasic.es/revista-sic-numero-152/