Universidad Tecnológica Nacional
AJEA – Actas de Jornadas y Eventos Académicos de UTN
Trabajo Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1c37
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Colección JIT en AJEA https://rtyc.utn.edu.ar/index.php/ajea/JITs

Jóvenes Investigadores Tecnológicos RAFAELA 2023
Facultad Regional Rafaela 26 y 27 de octubre de 2023

Área: Sistemas de información e informática / Categoría: Estudiante de Grado / Regional: Facultad Regional Rosario

Análisis de propuestas para detección de amenazas en tiempo real utilizando Inteligencia Artificial.

Analysis of approaches for Real-time Threat Detection using Artificial Intelligence.

Presentación: 17/10/2023

Bautista Guerra
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
bautistaguerra.it@gmail.com

Ornella Colazo
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
ornecolazo@gmail.com

Maximiliano Mansilla
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
mmansilla02@outlook.com

Guillermo Dolan
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
guillermopatdolan@gmail.com

Lucía Morena Fabbri
Universidad Tecnológica Nacional Facultad Regional Rosario Argentina
fabbriluciam@gmail.com

Resumen

Este trabajo se centra en analizar la utilización de técnicas de inteligencia artificial, específicamente el aprendizaje profundo, para mejorar la precisión y eficiencia en la detección de amenazas de ciberseguridad en tiempo real. El objetivo es explorar el potencial de aprovechar algoritmos avanzados de aprendizaje automático para identificar y clasificar diversos tipos de amenazas cibernéticas de manera oportuna. Además, el estudio tiene como propósito analizar la posible integración de esta capacidad mejorada de detección de amenazas en un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI) para cumplir con los objetivos del Proyecto "Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a sistemas de gestión de calidad" (Universidad Tecnológica Nacional – Facultad Regional Rosario, 2023) en que se encuadra este trabajo, de forma tal de poder lograr una gestión de riesgos más efectiva y fortalecer la postura de las organizaciones en torno a la Seguridad de la Información.

Palabras clave: inteligencia artificial, aprendizaje profundo, detección de amenazas, ciberseguridad.

Abstract

This research is dedicated to scrutinizing the utilization of artificial intelligence techniques, specifically deep learning, to enhance the accuracy and efficiency of real-time cybersecurity threat detection. The aim is to explore the potential of harnessing advanced machine learning algorithms for the timely identification and classification of various cyber threats. Furthermore, this study seeks

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

to assess the possible integration of this enhanced threat detection capability into an Information Security Risk Diagnosis System (ISRDS) to align with the objectives of the Project "Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a sistemas de gestión de calidad" (Universidad Tecnológica Nacional – Facultad Regional Rosario, 2023) within the scope of this research. This endeavor aims to achieve more effective risk management and bolster organizations' stance on Information Security.

Keywords: artificial intelligence, deep learning, threat detection, cybersecurity.

Introducción

En el contexto actual, caracterizado por el aumento constante en la frecuencia y sofisticación de los ataques cibernéticos (E. Rodriguez et al., 2021: 1920-1925), (I. H. Sarker et al., 2020: 1-29), la necesidad de adoptar enfoques avanzados para la detección y mitigación oportuna de estas crecientes amenazas en tiempo real se vuelve imperativa. A pesar de que los métodos tradicionales de detección han demostrado su eficacia en numerosos escenarios (A. L. Buczak and E.Guven, 2015: 1153-1176), (T. T. Nguyen and G. Armitage, 2008: 56-76), (M. Graczyk et al., 2009: 800-812), se enfrentan a desafíos significativos para mantenerse actualizados ante la constante evolución del panorama de amenazas. En este sentido, la inteligencia artificial (IA), en particular, el aprendizaje profundo (Deep Learning - DL), ha surgido como una estrategia prometedora para abordar estos retos en el campo de la ciberseguridad.

Este trabajo se centra en el análisis de la viabilidad de utilización de técnicas de inteligencia artificial, específicamente el aprendizaje profundo, con el objetivo de mejorar tanto la precisión como la eficiencia en la detección de amenazas cibernéticas en tiempo real. Se busca capitalizar el potencial de algoritmos avanzados de aprendizaje automático para identificar y clasificar diversas formas de amenazas cibernéticas de manera temprana. Además, se hace hincapié en la integración de esta capacidad mejorada de detección de amenazas en un Sistema de Diagnóstico de Riesgos de Seguridad de la Información (SDRSI), en concordancia con la justificación de nuestro proyecto (Riva, Fabiana María et al., 2022) y con las directrices de la norma ISO 27001:2022 - Sistema de Gestión de Seguridad de la información. Esta integración ofrecerá la posibilidad de fortalecer la gestión de riesgos y la postura general frente a la seguridad de la información de las organizaciones.

Para lograr estos objetivos, este trabajo realiza un análisis de la literatura existente y el estudio de investigaciones relevantes (E. Rodriguez et al., 2021), (N. Shon et al., 2018), (L. Mohammadpour et al., 2022), (J. Lansky et al., 2021), (M. A. Ferrag et al., 2020), (Z. Ahmad et al., 2021) con el propósito de proporcionar una visión de las técnicas y enfoques de vanguardia en la utilización del aprendizaje profundo para la detección de amenazas cibernéticas en tiempo real. Se aspira a subrayar los beneficios potenciales de combinar técnicas de inteligencia artificial, especialmente el aprendizaje profundo, con el enfoque dado al SDRSI. Al mejorar la detección y mitigación de amenazas, las organizaciones estarán mejor preparadas para salvaguardar activos críticos y datos confidenciales en un entorno digital cada vez más desafiante (I. H. Sarker et al., 2021: 1-18). Este estudio no solo busca abordar los desafíos actuales, sino también anticiparse a las amenazas futuras en un campo en constante evolución.

Amenazas cibernéticas: Fases de un ataque y Tipos de amenazas

Nuestro abordaje requiere introducir algunos conceptos esenciales, en principio, el concepto de ciberseguridad. **Ciberseguridad** comprende los procesos y herramientas utilizados para proteger la confidencialidad, integridad y disponibilidad (Confidentiality, Integrity and Availability – CIA), (S. Samonas and D. Coss, 2014), (D. Schatz et al., 2017) de los recursos y activos en el ciberespacio (E. Rodriguez et al., 2021).

Adicionalmente, en el ámbito de la ciberseguridad, una amenaza cibernética se refiere a cualquier evento o acción que tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad (S. Samonas and D. Coss, 2014) de los sistemas, datos

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

y activos digitales de una organización. Estas amenazas se materializan en ataques que son perpetrados por actores malintencionados o no, y tienen el efecto de explotar vulnerabilidades en los sistemas informáticos y obtener acceso no autorizado, causar daño o robar información sensible.

Las amenazas cibernéticas se materializan como procesos cuidadosamente planificados y ejecutados por atacantes con el objetivo de lograr sus fines maliciosos. Estos procesos se dividen en varias fases (T. Yadav and A. M. Rao, 2015: 438–452), (A. Shostack, 2014) cada una con su propio propósito y actividades específicas:

- **Investigación y recopilación de información:** los atacantes comienzan investigando su objetivo, identificando posibles vulnerabilidades, configuraciones débiles y brechas de seguridad. Utilizan herramientas y técnicas de búsqueda para recopilar información sobre sistemas, redes y empleados.
- **Adquisición de acceso:** una vez que se identifican las vulnerabilidades, los atacantes buscan formas de obtener acceso no autorizado. Esto puede involucrar la explotación de vulnerabilidades conocidas o el uso de ingeniería social para persuadir a los usuarios a proporcionar información de acceso.
- **Establecimiento de punto de apoyo:** los atacantes buscan mantener el acceso y la persistencia en el sistema comprometido. Pueden crear cuentas de usuario falsas, instalar malware persistente o modificar configuraciones para asegurarse de que puedan regresar y continuar su ataque en el futuro.
- **Desarrollo de objetivos:** en esta fase, los atacantes identifican sus objetivos específicos dentro del sistema comprometido. Esto podría incluir la búsqueda de datos confidenciales, la exfiltración de información valiosa o la alteración de datos.
- **Movimiento lateral:** los atacantes se mueven lateralmente a través de la red, escalando privilegios y buscando sistemas adicionales para comprometer. Esto les permite acceder a más recursos y datos valiosos.
- **Mantenimiento de acceso:** los atacantes continúan manteniendo su acceso y persistencia en el sistema comprometido. Esto puede implicar la actualización de herramientas maliciosas, el cambio de credenciales y la ocultación de su presencia.
- **Cumplimiento de objetivos:** en esta fase, los atacantes logran sus objetivos previamente definidos. Pueden robar información, causar daños, distribuir malware o llevar a cabo cualquier otra acción maliciosa que tenían en mente.
- **Retirada encubierta:** una vez que se ha logrado el objetivo, los atacantes pueden retirarse de manera encubierta para evitar la detección. Pueden eliminar rastros de su actividad maliciosa y ocultar su presencia en el sistema.

Detección de amenazas

Como posible medida para garantizar la protección de la tríada CIA (Confidencialidad, Integridad y Disponibilidad (Availability)), se puede optar por la implementación de un **Sistema de Detección de Intrusiones** (Intrusion Detection System - IDS). Para poder comprender qué es un IDS primero debemos tener en claro qué es una intrusión y qué realiza la detección de intrusiones. Acorde a (H.-J. Liao et al., 2013: 16-24) podemos definir a una **intrusión** como un intento de comprometer al menos una de las componentes de la tríada CIA, o eludir los mecanismos de seguridad de una computadora o red. Consecuentemente, entendemos a la **detección de intrusiones** como el proceso de monitorizar los eventos que ocurren en un sistema informático o red, y analizarlos en busca de signos de intrusiones, relacionadas con las Fases 1 a 3 de un ataque identificadas anteriormente. Una vez definidos estos conceptos podemos decir que un **IDS** es el sistema, tanto software como hardware, para automatizar el proceso de detección de intrusiones.

Distintos tipos de IDS

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

En general, nos encontraremos con dos criterios de clasificación para los distintos IDS. Conforme a (Z. Ahmad et al., 2021) clasificaremos a los distintos IDS dependiendo en dónde se implemente la detección de intrusiones o dependiendo del método utilizado para detectar las intrusiones.

En cuanto al criterio que depende de donde se implemente la detección de intrusiones podemos encontrar:

- **Host-based IDSs (HIDS):** realizan la monitorización de cada host y en caso de detectar actividad maliciosa alertan al usuario.
- **Network-based IDSs (NIDS):** realizan la monitorización de anomalías en el tráfico de la red ya que están situados en el nodo de la misma.

Es importante destacar que uno de los desafíos que enfrentan los HIDS radica en la necesidad de implementar el IDS en cada host que requiere protección contra intrusiones. Esta implementación puede generar una sobrecarga de procesamiento adicional en cada nodo, lo que en última instancia puede degradar el rendimiento del IDS (P. Kabiri and A. A. Ghorbani, 2005: 84-102). Sin embargo, se podría realizar un análisis más detallado y específico para evaluar adecuadamente la idoneidad de la implementación de técnicas de IA en el contexto de los HIDS. En consecuencia, este trabajo se centrará sólo en abordar la implementación de técnicas de detección de amenazas basadas en IA en el contexto de los NIDS.

Paralelamente, podemos clasificar a los distintos IDS dependiendo del método utilizado en la detección de intrusiones:

- **Signature-based intrusion detection systems (SIDS):** realizan la detección de ataques previamente conocidos basados en patrones predefinidos para actividades maliciosas dentro de una red.
- **Anomaly-based intrusion detection systems (AIDS):** realizan la detección de ataques novedosos o desconocidos basándose en la definición de patrones de comportamiento usuales e inusuales.

Utilizando SIDSs podemos lograr una alta precisión en la detección pero seremos incapaces de detectar ataques "novedosos", aquellos que escapen de los patrones predefinidos para actividades maliciosas dentro de una red. Por este motivo en este trabajo nos centramos en la utilización de AIDS los cuales, a pesar de proveer una precisión más baja, poseen la capacidad para detectar ataques de los cuales no se tiene registro.

Un IDS sirve como una herramienta de seguridad cibernética diseñada para monitorear constantemente el tráfico de red y los eventos del sistema en busca de patrones de actividad que puedan indicar intrusiones o comportamientos maliciosos. El funcionamiento básico de un IDS implica los siguientes pasos:

- **Captura de datos:** el IDS recopila datos de múltiples fuentes, como registros del sistema, tráfico de red y eventos de seguridad.
- **Análisis de datos:** utiliza algoritmos y reglas predefinidas para analizar los datos en busca de patrones sospechosos. Estos patrones pueden incluir firmas conocidas de ataques en el caso de los SIDS o anomalías en el tráfico de red si hablamos de un AIDS.
- **Detección de intrusiones:** si el IDS encuentra un patrón que coincide con una firma conocida o detecta un comportamiento anómalo, genera una alerta para notificar a los administradores del sistema.
- **Generación de alertas:** las alertas pueden ser notificaciones visuales, mensajes de correo electrónico o registros en un sistema centralizado de gestión de eventos y seguridad (SIEM).

Posteriormente a la implementación de un IDS, lo adecuado sería realizar acciones preventivas para mitigar el impacto de la amenaza detectada. Para lograr esto, es recomendable la implementación de un Sistema de Prevención de Intrusiones (Intrusion Prevention System - IPS) que puede considerarse como una extensión de un IDS que no solo detecta intrusiones, sino que también toma medidas activas para prevenirlas.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

Funcionamiento de un IPS

El proceso de funcionamiento de un IPS incluye:

- **Recepción de alertas:** el IPS recibe alertas generadas por el IDS o por sus propios sensores de detección. Estas alertas indican posibles intrusiones o actividades maliciosas.
- **Comparación y evaluación:** el IPS compara las alertas recibidas con su base de datos de firmas conocidas y reglas de seguridad. También evalúa la criticidad y el riesgo asociados con la alerta.
- **Acciones preventivas:** si la alerta se considera una amenaza válida y significativa, el IPS toma medidas activas para prevenir la intrusión. Estas acciones pueden incluir bloqueo de direcciones IP, cierre de puertos, reconfiguración de reglas de firewall, entre otras.
- **Generación de informes:** el IPS registra todas las acciones realizadas y genera informes detallados sobre las amenazas detectadas y las medidas preventivas tomadas.

De este modo, realizar una adecuada integración de un IPS con un IDS sería fundamental para lograr una detección de amenazas en tiempo real basada en aprendizaje profundo. El IDS detectaría actividades sospechosas utilizando técnicas de inteligencia artificial, como el aprendizaje profundo, y generaría alertas. El IPS, al recibir estas alertas, tomaría medidas preventivas para bloquear o mitigar las intrusiones en tiempo real. Esta integración contribuiría hacía un sistema más robusto y proactivo para la detección y prevención de amenazas. Al combinar la capacidad de detección precisa del IDS con las medidas de seguridad en tiempo real del IPS, se fortalece la postura de seguridad de la red o sistema, reduciendo el riesgo de intrusiones y ataques exitosos.

Integrar la detección de amenazas en tiempo real basada en inteligencia artificial con el SDRSI

Una de las estrategias fundamentales para lograr una detección efectiva de amenazas consiste en la implementación de un IDS y un IPS basados en inteligencia artificial, específicamente en técnicas de aprendizaje profundo. Como hemos visto, estas técnicas han demostrado su eficacia en el análisis y procesamiento de grandes volúmenes de datos, lo que resulta fundamental para identificar patrones y comportamientos anómalos asociados a actividades maliciosas.

En este sentido, el IDS, basado en algoritmos de aprendizaje profundo, tendrá la capacidad de analizar flujos de datos en tiempo real y detectar patrones y comportamientos anómalos asociados a actividades maliciosas o potencialmente riesgosas. Por otro lado, el IPS, estrechamente integrado con el IDS, tendrá la función de tomar medidas preventivas en tiempo real, bloqueando o mitigando las amenazas identificadas, con el objetivo de evitar posibles daños o vulnerabilidades en los sistemas y la información.

La integración de estos sistemas de inteligencia artificial con el SDRSI permitirá a las organizaciones una respuesta más rápida y eficiente ante incidentes de seguridad, lo que redundará en una disminución del tiempo de respuesta (Z. Ahmad et al., 2021), (P. Kabiri and A. A. Ghorbani, 2005: 84-102) y una mayor protección de la información sensible. Además, la retroalimentación continua y el aprendizaje automático de estos sistemas contribuirán a una mejora constante en la precisión de detección, lo que resulta crucial en un entorno en constante evolución de las amenazas cibernéticas.

La adopción de la Norma ISO 27001:2022 (“Iso 27001:2022 - information security, cybersecurity and privacy protection — information security management systems — requirements”, 2022) en Sistemas de Gestión de Seguridad de la Información proporcionará el marco normativo y los lineamientos necesarios para establecer políticas de seguridad, realizar evaluaciones de riesgos y definir controles apropiados definidos en la ISO 27002:2022 (“Iso 27002:2022 - information security, cybersecurity and privacy protection — information security controls”, 2022). En particular los conceptos analizados hasta aquí permiten avanzar en la implementación del control Inteligencia de las Amenazas incorporado en la última versión de la Norma y en evaluación por parte de nuestro proyecto “Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

sistemas de gestión de calidad" (Universidad Tecnológica Nacional – Facultad Regional Rosario, 2023), que servirá de base para el cumplimiento del objetivo de desarrollo del SDRSI.

La integración de sistemas basados en inteligencia artificial al SDRSI involucra varios pasos esenciales para garantizar una implementación efectiva y una mejora significativa en la detección de amenazas en tiempo real.

Una vez analizado el contexto organizacional, definidas las políticas de seguridad de la información y realizado el inventario de activos en base a los procesos documentados, fundamentos establecidos en la justificación de nuestro proyecto (Riva, Fabiana María et al., 2022), se deberán analizar algunos requisitos para la integración mencionada anteriormente:

- **Selección de herramientas:** Se debe determinar qué indicadores clave de riesgos (KRI) serán utilizados para la detección temprana de amenazas para así poder seleccionar las herramientas y tecnologías adecuadas para la implementación del IDS y el IPS basados en inteligencia artificial (I. H. Sarker et al., 2021: 1-18), (A. Patel et al., 2010).
- **Entrenamiento y aprendizaje continuo:** se deberá proceder al entrenamiento y aprendizaje continuo de los algoritmos de inteligencia artificial utilizados en el IDS y el IPS. El entrenamiento inicial es esencial para que los algoritmos puedan aprender de los datos históricos y desarrollar modelos precisos de detección de amenazas. Sin embargo, como se mencionó anteriormente la ciberseguridad es un campo en constante evolución, por lo que el aprendizaje debe ser continuo para mantenerse al día con las nuevas amenazas y patrones de ataque. Es por ello que este trabajo se centra en la implementación de AIDS para poder detectar ataques de los cuales no se tiene registro.
- **Integración del IDS y IPS al SDRSI:** esta integración implica la sincronización de los sistemas, de manera que la información y datos relevantes para la detección de amenazas sean compartidos entre ellos de manera eficiente y segura (A. L. Mesquida et al., 2010) y se establezcan mecanismos de comunicación efectivos, de manera que el IDS pueda recibir información en tiempo real sobre los activos críticos y los indicadores clave de riesgos (KRI) del SDRSI, y el IPS pueda tomar acciones preventivas o correctivas en caso de detectar amenazas.
- **Monitoreo y evaluación del desempeño:** esta evaluación periódica del desempeño del SDRSI y los sistemas de inteligencia artificial permitirá identificar posibles mejoras y ajustes necesarios, estableciendo indicadores clave de desempeño (KPI), para garantizar una detección de amenazas óptima y una respuesta efectiva ante incidentes de seguridad.

Adoptando esta metodología podemos obtener una solución integral y proactiva para la gestión de la seguridad de la información en el ámbito de la Industria del Software y Servicios Informáticos, abordando las demandas actuales de ciberseguridad y adaptándose a las exigencias de un entorno digital en constante cambio. La integración de la Inteligencia Artificial al SDRSI representará un paso significativo hacia la mejora continua de la seguridad y la calidad, fortaleciendo la posición competitiva de estas organizaciones y contribuyendo a la confianza y satisfacción de sus clientes.

Conclusiones

A lo largo de este trabajo, se ha explorado la convergencia de elementos fundamentales para garantizar la ciberseguridad en entornos empresariales. La integración del IDS y el IPS con el SDRSI representa una posibilidad de abordaje en la detección de las complejas amenazas cibernéticas de hoy en día.

La aplicación de técnicas de aprendizaje profundo agrega un nivel significativo de sofisticación a la detección de amenazas. Al aprovechar algoritmos avanzados, como redes neuronales convolucionales y recurrentes, se logra una detección más precisa y adaptativa. El aprendizaje profundo permite el análisis en tiempo real de grandes volúmenes de datos, identificando patrones sutiles y anomalías que podrían pasar desapercibidas por métodos tradicionales.

La fortaleza de la integración de estas técnicas al SDRSI planteado radica en su capacidad para no solo anticipar y detectar, sino también responder de manera automática a las amenazas. Esta característica es crucial para reducir el tiempo de respuesta ante

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

incidentes y mitigar el impacto potencial. Al combinar la detección precisa de IDS y la acción proactiva de IPS, respaldadas por la inteligencia de riesgos del SDRSI, las organizaciones están mejor equipadas para salvaguardar su entorno digital.

Reconocimientos y agradecimientos

El presente trabajo fue realizado en el contexto del proyecto: TOECRO0008583 - 'Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información para su Integración a Sistemas de Gestión de Calidad' (Universidad Tecnológica Nacional – Facultad Regional Rosario, 2023).

Agradecemos a nuestro equipo de Investigación conformado por docentes y alumnos que siempre están dispuestos para las dudas que nos van surgiendo y para asesorarnos con la experiencia que ellos poseen.

Referencias bibliografías

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150.

Boukra, W. G. A. (2017). GAB-BBO: adaptive biogeography-based feature selection approach for intrusion detection. *International Journal of Computational Intelligence Systems, 10*, 914-935.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials, 18(2),* 1153-1176.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

Graczyk, M., Lasota, T., & Trawiński, B. (2009). Comparative analysis of premises valuation models using KEEL, RapidMiner, and WEKA. In *Computational Collective Intelligence. Semantic Web, Social Networks and Multiagent Systems: First International Conference, ICCCI 2009, Wrocław, Poland, October 5-7, 2009. Proceedings 1* (pp. 800-812). Springer Berlin Heidelberg.

Iso 27001:2022 - information security, cybersecurity and privacy protection — information security management systems — requirements, no. 2, 2022.

Iso 27002:2022 - information security, cybersecurity and privacy protection — information security controls, no. 2, 2022.

Kabiri, P., & Ghorbani, A. A. (2005). Research on intrusion detection and response: A survey. *Int. J. Netw. Secur., 1*(2), 84-102.

Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE Access, 9*, 101574-101599.

L. Mohammadpour, T. C. Ling, C. S. Liew, y A. Aryanfar, “A survey of cnn-based network intrusion detection,” *Applied Sciences*, vol. 12, no. 16, p. 8162, 2022.

AJEA – Actas de Jornadas y Eventos Académicos de UTN
Libro de actas de resúmenes DOI: https://doi.org/10.33414/ajea.1640.2024
Texto Completo Publicado en AJEA – Full Text Published in AJEA
https://rtyc.utn.edu.ar/index.php/ajea/article/view/1637

Mesquida, A. L., Mas, A., Amengual, E., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS. *Revista Española de Innovación, Calidad e Ingeniería del Software, 6*(3), 25-34.

Nguyen, T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning*. IEEE communications surveys & tutorials, 10(4),* 56-76.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security, 18*(4), 277-290.

Proyecto: Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a sistemas de gestión de calidad). Código: TOE-CRO0008583 Vigencia: Del 1/4/2023 al 31/03/2025. Universidad Tecnológica Nacional – Facultad Regional Rosario.

Riva, F. M., Maenza, R. R., Pereira, N., Font, G., Martin, V., Fabbri, L., Dolan, G., Butti, J., & Bidart, F. "Modelización de un sistema de riesgos de seguridad de la información (SDRSI) para su integración a sistemas de gestión de calidad," *En memorias: CONAIISI 2022.10mo Congreso Nacional de Informática e Ingeniería en Sistemas de Información. UTN Facultad Regional Concepción del Uruguay. Publicación on line – ISBN 978-950-42-0218-9*, 2022

Rodriguez, E., Otero, B., Gutierrez, N., & Canal, R. (2021). A survey of deep learning techniques for cybersecurity in mobile networks. *IEEE Communications Surveys & Tutorials, 23(3),* 1920-1955.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data, 7*, 1-29.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science, 2*, 1-18.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3).

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 8.

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence, 2*(1), 41-50.

Shostack, A. (2014). Threat modeling: Designing for security. *John Wiley & Sons.*

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access, 5*, 21954-21961.

Yadav, T. y Rao, A. M. Technical aspects of cyber kill chain. *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3*, pp. 438–452, Springer, 2015.