# Uso de técnicas de Machine Learning para la Detección Temprana de Ransomware

Gonzalo Heinen, Mayra Alejandra Milano , Jorge Kamlofsky
*CAETI - Centro de Altos Estudios en Tecnología Informática.*
*Universidad Abierta Interamericana, Facultad de Tecnología Informática*

***Abstract***
*Se explora el impacto de la convergencia entre redes de Tecnología Operacional (OT) y de Tecnologías de la Información (IT) en infraestructuras críticas, poniendo especial énfasis en la vulnerabilidad de los sistemas SCADA ante la creciente amenaza de los Ransomware. Para enfrentar este desafío, se describe un experimento que evalúa la capacidad de algoritmos de aprendizaje automático (Machine Learning) para detectar actividades maliciosas en fases tempranas de un ataque, antes de que el malware logre propagarse o cifrar datos críticos. Mediante la simulación de un entorno de red que integra componentes IT y OT de forma realista, se busca demostrar la eficacia de técnicas de análisis de comportamiento y de identificación de patrones anómalos para reforzar la seguridad de sistemas industriales estratégicos y mitigar el impacto de incidentes cibernéticos.*

***Palabras clave****: Infraestructuras críticas, Ciberseguridad, Redes OT, Sistemas SCADA, Ransomware, Machine Learning, Convergencia IT/OT.*

## INTRODUCCIÓN

Las infraestructuras críticas desempeñan un papel fundamental en la estabilidad, la seguridad y el desarrollo de un país, puesto que abarcan sectores esenciales como la energía, el transporte, las telecomunicaciones y los servicios de defensa. En este contexto, las redes de Tecnología Operacional (OT), responsables de gestionar y controlar sistemas físicos en dichos ámbitos, han adquirido una relevancia estratégica ante la creciente necesidad de protegerlas frente a amenazas cibernéticas avanzadas [1].

La Reciente Directiva de Política de Defensa Nacional [1] enfatiza la importancia de la protección de infraestructuras estratégicas, destacando que el Sistema de Defensa Nacional debe enfocarse en la seguridad de aquellas infraestructuras cuyo funcionamiento resulta crítico para el ejercicio de la soberanía y el resguardo de la vida y libertad de los ciudadanos. En este sentido, diversas instituciones académicas y organismos de ciberseguridad han impulsado proyectos orientados a fortalecer la resiliencia de las infraestructuras OT [2], mediante el desarrollo de herramientas avanzadas de detección y respuesta ante incidentes de ciberseguridad.

En Argentina, el Ejército Argentino (EA) ha promovido el desarrollo de sistemas de comando y control (SC2) para sus brigadas, lo que ha dado lugar a una mayor interconexión y automatización de estos sistemas. Sin embargo, esta evolución también ha incrementado la superficie de ataque y la vulnerabilidad frente a amenazas cibernéticas, lo que ha motivado la creación de proyectos como la propuesta de InFoscopia [3].

Por otro lado, el Comando Conjunto de Ciberdefensa ha trabajado en la consolidación de capacidades de ciberdefensa y respuesta ante incidentes en infraestructuras críticas industriales (ICI) [4], a través de proyectos como el Programa

de Desarrollo Tecnológico-Social (PDTS)[1], que ha contado con el apoyo de diversas universidades e instituciones gubernamentales y privadas.

La relevancia de estos proyectos radica en la creciente sofisticación de los ataques a sistemas OT, que van desde la interrupción de procesos industriales hasta el secuestro de sistemas mediante ransomware y la explotación de vulnerabilidades en dispositivos Supervisory Control And Data Acquisition (SCADA).

En este contexto el objetivo del presente trabajo es el contextualizar la vulnerabilidad de los sistemas SCADA y presentar un experimento de alcance limitado que evalúe la capacidad del uso de machine learning para detectar posibles atacantes durante la fase de pre-ataque, contribuyendo así a prevenir ataques de ransomware en redes OT.

## 1. Convergencia entre redes IT y OT

A medida que las redes de Tecnologías de la Información (IT) y OT convergen para mejorar la eficiencia y la productividad de entornos industriales, surgen desafíos significativos en materia de ciberseguridad. Tradicionalmente, los sistemas OT funcionaban de manera aislada y estaban diseñados para operar con un énfasis casi absoluto en la disponibilidad y la seguridad física de los procesos. Por su parte, en IT se han consolidado múltiples mecanismos para proteger datos, redes y servidores frente a ataques cibernéticos. Cuando ambas dimensiones se integran, la confluencia de requisitos tan distintos provoca vulnerabilidades que ponen en riesgo la confiabilidad e incluso la seguridad de instalaciones críticas.

La amenaza del ransomware ha experimentado un crecimiento exponencial en sistemas de control industrial y otras infraestructuras críticas [6]. Este tipo de ataque, que cifra datos o inutiliza dispositivos a cambio de un rescate, ha pasado de afectar principalmente a la capa IT a propagarse cada vez más en entornos OT. La conectividad creciente de plantas industriales y la adopción de protocolos sin suficientes medidas de cifrado o autenticación ha facilitado que los atacantes encuentren nuevas vías de acceso a sistemas de supervisión y control. Tal expansión eleva el riesgo de interrupción de procesos esenciales, con consecuencias potencialmente graves en términos de producción y seguridad física.

En primer lugar, el hecho de que los dispositivos industriales (como PLC, controladores de proceso o RTU) se conecten a redes IP comunes amplía la superficie de ataque. Muchos protocolos tradicionales de campo (por ejemplo, Modbus o PROFIBUS) se diseñaron sin cifrado o autenticación adecuados, pues su objetivo original era la operación confiable y en tiempo real de procesos físicos, no la protección frente a ataques. Al migrar estos protocolos a variantes sobre TCP/IP (Modbus/TCP o PROFINET, entre otros), se heredan carencias de seguridad difíciles de remediar sin rediseñar los dispositivos o invertir en soluciones de encapsulación y monitoreo especializado.

La separación entre la red corporativa IT y la red de planta OT se ha ido diluyendo. Muchas organizaciones requieren visualizar datos de producción en tiempo real en sistemas empresariales o en la nube, lo que facilita la toma de decisiones basadas en grandes volúmenes de datos (Big Data y IIoT). Sin embargo, estos enlaces cruzados, si no se gestionan con cautela, permiten que ataques originados en la capa IT —por ejemplo, mediante correos de phishing o exploits conocidos para sistemas Windows— se propaguen hasta los equipos

[1] Decreto 703/2018. DECTO-2018-703-APN-PTE - Directiva de Política de Defensa Nacional.

[2] Proyectos de desarrollo tecnológico y/o de impacto social.

de control industrial. A la luz de la escalada de casos de ransomware mencionada, esta interconexión se convierte en un factor crítico que agrava la exposición de los activos OT [5].

## 2. FASES DE ATAQUE DE UN RANSOMWARE

Las fases de un ataque de ransomware comienzan antes incluso de la ejecución del malware en los sistemas de la víctima. En esta etapa de pre-ataque, los ciberdelincuentes llevan a cabo labores de reconocimiento y obtención de información, conocidas como reconocimiento (reconnaissance) en la Cyber Kill Chain. Durante esta fase preliminar, los atacantes identifican posibles vulnerabilidades en los sistemas de la organización, recopilan credenciales filtradas en la dark web, estudian qué servicios están expuestos a Internet e investigan las medidas de seguridad implementadas. Asimismo, pueden preparar herramientas de acceso inicial como troyanos o correos de phishing que servirán para la fase de entrega (delivery), cuidando la furtividad de sus métodos y adaptando sus tácticas según el perfil de la víctima.

Una vez logrado el acceso, los atacantes se enfocan en escalar privilegios, moverse lateralmente por la red y establecer persistencia en los sistemas comprometidos. Para ello, pueden emplear técnicas como exploits conocidos para servidores o el uso de credenciales robadas. Completado este movimiento interno, se pasa a la fase de impacto o ataque directo, en la que el ransomware cifra ficheros críticos y, a menudo, exfiltra datos sensibles para ejercer presión (doble extorsión). Finalmente, la víctima recibe la nota de rescate en la que se detalla el pago exigido para restaurar sus datos o evitar su publicación [7].

## 3. MACHINE LEARNING PARA LA DETECCIÓN DE UN RANSOMWARE

La implementación de técnicas de Machine Learning para la detección de ransomware podría representar un paso relevante en la búsqueda de soluciones más adaptables y robustas para proteger infraestructuras informáticas. Se cree que, al emplear algoritmos como Random Forest, Naïve Bayes o Support Vector Machine, se lograría analizar patrones de comportamiento en archivos o procesos que, tradicionalmente, pasan inadvertidos en enfoques basados únicamente en firmas o reglas fijas. De concretarse, dichos modelos tendrían la capacidad de aprender continuamente de nuevos ataques, ampliando su eficacia frente a variantes más recientes de malware y, en particular, de ransomware.

Sin embargo, la implementación de esta solución presenta problemas. Uno de los principales es el costo/beneficio de la implementación de un hardware lo suficientemente potente para emplear el machine learning de forma óptima e inmediata [8].

## 4. LÍNEAS DE INVESTIGACIÓN Y EXPERIMENTO EN REDES IT/OT

En el marco del proyecto de Ciberdefensa en redes OT del CAETI, el objetivo es estructurar un experimento diseñando una infraestructura de red interna que emula de manera realista las condiciones y registros característicos de un entorno de oficina, con el fin de estudiar y anticipar amenazas de tipo ransomware. Para ello, se han dispuesto dos segmentos de red (IT y OT) tal como se aprecia en las topologías, donde cada

segmento aloja diversos equipos y servicios comunes en ambientes corporativos (por ejemplo, servidores, puestos de trabajo y dispositivos de automatización). Este montaje controlado posibilita la captura y el análisis de eventos de manera más fidedigna, reflejando con mayor precisión la actividad esperable en escenarios de producción.

Bajo este contexto, la intención es aplicar en la siguiente etapa del experimento técnicas de inteligencia artificial, concretamente de aprendizaje automático (Machine Learning), para revisar sistemáticamente los registros y flujos de datos generados en la red. De esta manera, se espera identificar patrones de comportamiento anómalo asociados con un potencial ataque de ransomware, particularmente desde la fase de pre-ataque. En última instancia, el objetivo consiste en validar la capacidad de un modelo automatizado para reconocer señales tempranas de infección antes de que el malware logre propagarse y comprometer los sistemas críticos, tanto en redes IT/OT separadas como unificadas.

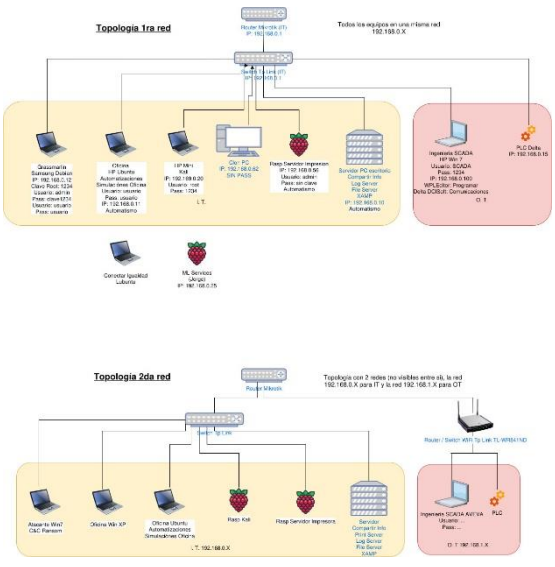


Figura 1. “TOPOLOGÍA DE REDES 1 Y 2”

Se observan las topologías de redes empleadas para dos casos de estudios distintos. En el primer caso la red OT se encuentra en convergencia con la red IT, mientras que en el segundo se encuentran por separado.

## 5. FORMACIÓN DE RECURSOS HUMANOS

El presente proyecto se encuentra dirigido por el Mg. Lic. Jorge Kamlofsky quien está cursando un Doctorado. Los resultados colaborarán con el desarrollo de su Tesis.
Para el desarrollo de las actividades está prevista la participación de dos estudiantes de grado de la Universidad Abierta Interamericana de la carrera de grado de Ingeniería en Sistemas de información.
Por otro lado, el presente proyecto se enmarca como una de las líneas de trabajo que viene desarrollando el Laboratorio CAETI de la Universidad, en donde alumnos de grado y posgrado realizan sus trabajos finales de carrera. Por lo tanto, está prevista la incorporación de dos alumnos de grado y posgrado, quienes profundizarán sus saberes y realizarán los aportes correspondientes.

## 6. BIBLIOGRAFÍA

[1]: Giorgio Valenziano Santangelo y Vincenzo Giuseppe Colacino, “Analysis, prevention and detection of ransomware attacks on Industrial Control Systems”, Conference: 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)

[2]: Jorge Kamlofsky, Hugo Colombo, Claudio Milioy Pedro Hecht. “Ciberdefensa en Sistemas Operacionales”. Workshop de Investigadores en Ciencias de la Computación WICC 2024.

[3]: Liporace, Julio César, Buscaglia, Adrián, Croci, Pablo, Díaz Pais, Nicolás, Fernández, Darío, Ferreyra, Verónica, Gallardo Urbini, Ignacio Martín, Quiroga, Elvira, Vera Batista, Fernando, Cicerchia, César D. “Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional –infoscopia–“. Tecnología Workshop de Investigadores en Ciencias de la Computación WICC 2019

[4]: Kamlofsky, Jorge, Gonzalez, Gerardo, Trigo, Santiago “Infraestructuras Críticas Industriales ICI”. Workshop de Investigadores en Ciencias de la Computación WICC 2021.

[5]: Georgios Michail Makrakis, Constantinos Kolias, Georgios Kambourakis, Craig Rieger, Jacob Benjamin," Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures", Cornell University 10 Sep 2021.

[6]: Waterfall. "Industrial Cybersecurity" 2024.

[7]: Ramón José Paniagua Soza. Anatomía del ransomware. Junio 2022 Recuperado el 21 de febrero del 2025.