2025

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Ciber estrategia y Ciber Inteligencia

FUNDAMENTOS, APLICACIONES Y RETOS PARA LA RESILIENCIA EN ENTORNOS DIGITALES

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número treinta y cuatro [34]
Julio de 2025

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder Programa de Maestría en Ciberseguridad

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Desarrollo Tecnológico CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Adm. Libardo Cárdenas Corral
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Introducción

La creciente digitalización de los procesos sociales, económicos y políticos ha transformado el ciberespacio en un escenario estratégico donde confluyen oportunidades y amenazas. En este contexto, la ciberinteligencia se ha consolidado como una disciplina fundamental para anticipar, detectar y responder de manera efectiva a los riesgos derivados de actores hostiles y dinámicas adversariales que impactan a individuos, organizaciones e infraestructuras críticas. A diferencia de la ciberseguridad reactiva, que actúa frente a los incidentes una vez ocurren, la ciberinteligencia plantea un enfoque proactivo y preventivo, basado en la recolección, procesamiento y análisis de información proveniente de múltiples fuentes digitales. Su objetivo es convertir datos dispersos en conocimiento estratégico, capaz de guiar decisiones de alto impacto en la protección de activos digitales y en la construcción de resiliencia frente a amenazas emergentes. En el plano académico y profesional, la ciberinteligencia ha adquirido especial relevancia en los últimos años, gracias al desarrollo de metodologías estructuradas y la integración de tecnologías avanzadas como el aprendizaje automático y la inteligencia artificial(Alevizos & Dekker, 2024a). Estas innovaciones han potenciado la capacidad de las organizaciones para identificar patrones de ataque, anticipar vulnerabilidades y fortalecer la capacidad de respuesta en entornos cada vez más complejos e interconectados.

Sin embargo, más allá de las herramientas, la ciberinteligencia supone un cambio cultural: implica reconocer que la seguridad informática no depende únicamente de la implementación de controles técnicos, sino también de la gestión estratégica de la información. Así, marcos internacionales como MITRE ATT&CK[1], Cyber Kill Chain[2] y los desarrollos normativos nacionales (por ejemplo, CONPES 3701 de Ciberseguridad y Defensa, 2011[3]) subrayan la necesidad de integrar la inteligencia digital en la toma de decisiones a nivel directivo y operativo.

Este boletín presenta un recorrido cuatro ejes temáticos: los fundamentos de la ciberinteligencia como pilar estratégico de la seguridad digital; las metodologías y técnicas avanzadas de recolección de información; la producción de inteligencia estratégica como apoyo a la toma de decisiones; y los retos emergentes para la resiliencia en entornos digitales.

[1] https://attack.mitre.org/
[2] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[3] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Ciber Estrategia y Ciber Inteligencia

FUNDAMENTOS, APLICACIONES Y RETOS PARA LA RESILIENCIA EN ENTORNOS DIGITALES

Autores

Luis Fernando Zambrano Hernandez
Docente Investigador
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

Hernando José Peña Hidalgo
Docente Investigador
CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-3477-2645

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-0392-1983

Néstor Raúl Cárdenas Corral
Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: orcid.org/0000-0003-3691-0148

Ciberinteligencia como pilar estratégico en la seguridad digita

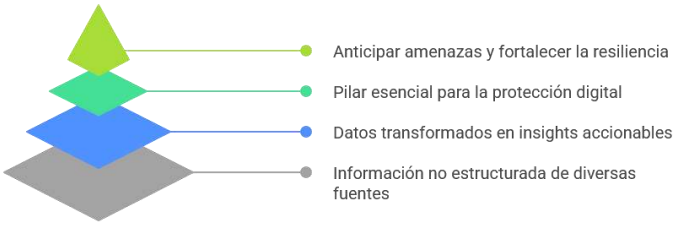
En el marco de la transformación digital, la ciberinteligencia ha emergido como un componente esencial para garantizar la protección de infraestructuras críticas, organizaciones y ecosistemas sociales cada vez más interconectados. A diferencia de la ciberseguridad tradicional, que suele centrarse en la reacción a incidentes ya ocurridos, la ciberinteligencia propone un enfoque de anticipación y estratégico, orientado a identificar amenazas, actores y patrones de ataque antes de que estos se materialicen.

Su importancia radica en la capacidad de convertir datos fragmentados en conocimiento accionable, lo que permite a los tomadores de decisión en materia de seguridad informática diseñar medidas preventivas, optimizar la asignación de recursos y fortalecer la resiliencia institucional. En este sentido, autores como (Irfan et al., 2022a) han propuesto una *taxonomía de marcos de inteligencia de amenazas* que clasifica los procesos de ciberinteligencia en función de su alcance, utilidad y aplicabilidad en entornos organizacionales, resaltando la necesidad de contar con estructuras sistemáticas y escalables para producir inteligencia digital(Irfan et al., 2022b)

El desarrollo de la ciberinteligencia también está vinculado a la evolución de las fuentes y técnicas de obtención de información. En este aspecto, Böhm y Lolagar (2021) destacan que el Open Source Intelligence (OSINT) se ha consolidado como una de las metodologías más valiosas para la recolección de datos en contextos digitales, no solo por su costo reducido, sino también por el amplio espectro de información disponible en la web superficial, profunda y oscura. Los autores advierten, sin embargo, que el uso de estas fuentes implica retos éticos y legales que deben ser atendidos con marcos regulatorios claros y políticas de gobernanza (Böhm & Lolagar, 2021). Por otro lado, la incorporación de tecnologías, como la inteligencia artificial y el aprendizaje automático, está transformando el campo de la ciberinteligencia. Según Alevizos y Dekker (2024), la integración de algoritmos de IA en los *pipelines*[4] de procesamiento de inteligencia permite automatizar la identificación de patrones y anomalías en grandes volúmenes de datos, lo que incrementa la capacidad de detección temprana de ataques y facilita la toma de decisiones basadas en evidencia. No obstante, también plantean la necesidad de garantizar transparencia y confiabilidad en el uso de estos sistemas (Alevizos & Dekker, 2024b)

En conjunto, estas perspectivas muestran que la ciberinteligencia no debe entenderse como un complemento opcional de la ciberseguridad, sino como un pilar estratégico que articula procesos técnicos, organizativos y normativos para anticipar riesgos, optimizar respuestas y generar confianza digital en la sociedad. Su valor radica no solo en proteger sistemas, sino también en consolidar la resiliencia digital como un activo estratégico para las organizaciones contemporáneas

Ilustración 1. Proceso de transformación de la información en el marco de la ciberinteligencia.



Napkin AI. (2025). *Proceso de transformación de la información en el marco de la ciberinteligencia* [Infografía generada con inteligencia artificial]. Napkin. https://app.napkin.ai/

[4] Un pipeline de Inteligencia Artificial es un flujo de trabajo estructurado que automatiza y estandariza todas las fases de desarrollo de modelos de IA.

Metodologías y técnicas de recolección de información digital

El proceso de ciberinteligencia se sustenta en la capacidad de recolectar información de diversas fuentes, tanto abiertas como cerradas, con el fin de identificar actores, tácticas y patrones de ataque. En este sentido, las metodologías y técnicas de obtención de información digital han evolucionado para responder a un panorama de amenazas cada vez más complejo.

El Open Source Intelligence (OSINT) constituye uno de los enfoques más relevantes en la actualidad. Según Böhm y Lolagar (2021), OSINT se ha convertido en una práctica esencial para las organizaciones, ya que permite acceder a información pública de alto valor estratégico. Sin embargo, los autores advierten que este proceso debe realizarse bajo principios éticos y legales claros, para evitar vulneraciones a la privacidad y garantizar la validez de las fuentes. (Böhm & Lolagar, 2021)

En paralelo, el Social Media Intelligence (SOCMINT)[5] ha adquirido relevancia en un mundo hiperconectado. Biagio et al. (2021) proponen un marco metodológico de SOCMINT que permite extraer datos de redes sociales para enriquecer procesos de inteligencia de amenazas. Su estudio demuestra que las plataformas sociales constituyen un canal fundamental para la detección temprana de campañas de desinformación, movimientos hacktivistas y posibles ciberataques. (Biagio et al., 2021).

Otra vertiente clave es el Signals Intelligence (SIGINT)[6], orientada a la captura y análisis de señales de comunicación. En el ámbito de la ciberinteligencia, el SIGINT se aplica a la detección de patrones en tráfico de red y comunicaciones cifradas. Aunque menos explorado en el contexto civil, representa un complemento necesario al OSINT y SOCMINT para la protección de infraestructuras críticas. Paya-Santos y Luque-Juárez (2021) resaltan que el SIGINT, junto con técnicas de inteligencia criminal, constituye un instrumento indispensable frente a amenazas transnacionales en el ciberespacio. (Paya-Santos & Luque-Juárez, 2021)

La dark web emerge como un espacio donde se comercializan credenciales robadas, herramientas de ataque y servicios ilícitos. La investigación de Yamin et

[5] Técnicas, tecnologías y herramientas que permiten la recopilación y el análisis de información de las plataformas de redes sociales

[6] Disciplina de la inteligencia militar y de ciberseguridad que se centra en la recolección, análisis e interpretación de señales electromagnéticas con el fin de obtener información estratégica, táctica o técnica.

al. (2022) propone un mapeo de herramientas OSINT enlazadas al modelo de la *Cyber Kill Chain*, destacando la importancia de monitorear foros y mercados clandestinos para anticipar ataques y comprender la lógica adversarial(Yamin et al., 2022)

Finalmente, los avances en inteligencia artificial están potenciando la recolección automatizada de información. Tang y Qiu (2022) desarrollaron un modelo de identificación automática de *Indicators of Compromise (IoCs)* basado en aprendizaje profundo, que permite acelerar la detección de amenazas en grandes volúmenes de datos provenientes de diversas fuentes, incluyendo OSINT y dark web. Esta contribución refuerza el papel de la IA en la optimización de procesos de ciberinteligencia(Tang & Qiu, 2022).

En conjunto, estas metodologías — OSINT, SOCMINT, SIGINT y el análisis de la dark web constituyen un entramado esencial para la construcción de ciberinteligencia robusta. Lo anterior, al integrarse con tecnologías emergentes, ofrecen a las organizaciones la posibilidad de anticiparse a ataques, comprender mejor a los adversarios y fortalecer su resiliencia frente a un ecosistema de amenazas en constante evolución.

Ilustración 2. Dimensiones de la Ciberinteligencia y sus Enfoques Clave

Napkin AI. (2025). *Dimensiones de la ciberinteligencia y sus enfoques clave* [Infografía generada con inteligencia artificial]. Napkin. https://app.napkin.ai/

Producción de inteligencia estratégica y toma de decisiones organizacionales

La producción de inteligencia estratégica constituye la fase en la que la información recolectada y procesada se transforma en productos de valor que sirven como soporte a la toma de decisiones. Estos productos pueden tomar la forma de informes ejecutivos, matrices de riesgos, alertas tempranas o dashboards de ciberinteligencia. Su objetivo principal es traducir los hallazgos técnicos en insumos comprensibles y accionables para los diferentes niveles de una organización, desde los analistas operativos hasta la alta dirección.

En esta línea, Sushama Pawar et al. (2024) presentan una revisión integral sobre la implementación práctica de la Cyber Threat Intelligence (CTI), destacando que la utilidad real de la inteligencia depende de su capacidad para integrarse en procesos de gestión y planificación estratégica. Los autores subrayan la importancia de generar productos diferenciados según el público objetivo: informes técnicos para equipos de SOC/CSIRT y reportes ejecutivos para directivos(Sushama Pawar et al., 2024)

La aplicación de técnicas de análisis predictivo se ha convertido en otro de los pilares de la producción de inteligencia. Yeboah-Ofori et al. (2021) proponen un modelo de análisis predictivo para la seguridad de cadenas de suministro, basado en CTI. Este enfoque permite anticipar vulnerabilidades y ataques antes de que se materialicen, reforzando la idea de que la inteligencia estratégica no se limita al diagnóstico, sino que impulsa decisiones preventiva(Yeboah-Ofori et al., 2021)

Desde una perspectiva más enfocada en la resiliencia, Ramírez Quevedo (2024) examina las tecnologías de defensa frente a la inteligencia de amenazas, enfatizando la necesidad de convertir los resultados de la ciberinteligencia en planes de acción concretos que fortalezcan la capacidad de las organizaciones para adaptarse y recuperarse ante ataques(Ramírez Quevedo, 2024)

La inteligencia estratégica también demanda un marco normativo que regule su producción y uso. En este sentido, Rejas de la Peña et al. (2025) analizan cómo la ciberinteligencia puede emplearse para reducir riesgos en activos críticos nacionales, resaltando la importancia de articular productos de inteligencia con políticas de seguridad pública y defensa nacional (Caballero-Delgadillo et al., 2025).

Finalmente, **Alevizos y Dekker (2024)** aportan una visión innovadora al describir cómo la inteligencia artificial puede mejorar el *pipeline* de procesamiento de inteligencia, generando productos estratégicos más rápidos y precisos. Su propuesta incluye la automatización de informes y la integración de modelos de IA para apoyar la toma de decisiones en tiempo real, ampliando así el impacto organizacional de la ciberinteligencia (Alevizos & Dekker, 2024b)

Ilustración 3. Impacto y Aplicaciones de la Inteligencia Estratégica

Napkin AI. (2025). *Impacto y aplicaciones de la inteligencia estratégica* [Infografía generada con inteligencia artificial]. Napkin. https://app.napkin.ai/

La imagen sintetiza los principales beneficios que aporta la inteligencia estratégica en el ámbito organizacional:

- Productos estratégicos: los datos se convierten en informes, alertas y tableros de control que apoyan la planeación y la toma de decisiones.
- Toma de decisiones guiada: la inteligencia estratégica provee información clave para orientar decisiones en todos los niveles de la organización.
- Protección de activos: su implementación contribuye a resguardar organizaciones y activos críticos, fortaleciendo la resiliencia frente a amenazas.

Conclusiones

La revisión de los fundamentos, metodologías y aplicaciones de la ciberinteligencia permite afirmar que esta disciplina constituye hoy un pilar estratégico de la seguridad digital, dado que facilita la anticipación de amenazas y la formulación de planes proactivos de protección en organizaciones públicas y privadas.

En primer lugar, la ciberinteligencia se configura como un proceso que trasciende la seguridad reactiva, transformando datos dispersos en conocimiento estratégico que aporta a la resiliencia digital. Esto implica que los profesionales de la seguridad informática no solo deben dominar herramientas técnicas, sino también marcos analíticos y normativos que les permitan generar productos útiles para la toma de decisiones.

En segundo lugar, las metodologías de recolección de información digital (OSINT, SOCMINT, SIGINT y análisis de la dark web) constituyen la base operativa de la ciberinteligencia. Su integración, junto con tecnologías emergentes como la inteligencia artificial y el aprendizaje automático, ofrece nuevas oportunidades para detectar amenazas de manera temprana. Sin embargo, también plantean retos éticos y legales que deben ser gestionados responsablemente.

En tercer lugar, la producción de inteligencia estratégica es la fase en la que el valor de la ciberinteligencia se concreta. Informes ejecutivos, dashboards, matrices de riesgos y alertas tempranas no son fines en sí mismos, sino instrumentos para orientar decisiones y acciones de mitigación. Su impacto se refleja tanto en la seguridad de los ecosistemas organizacionales como en la protección de infraestructuras críticas nacionales.

Finalmente, se evidencia que los retos actuales de la ciberinteligencia están ligados a la capacidad de las organizaciones para integrar los hallazgos técnicos en la estrategia corporativa. Ello implica adoptar un enfoque interdisciplinar que articule tecnología, normatividad y gestión, promoviendo la construcción de resiliencia digital frente a un entorno de amenazas dinámico y en constante evolución.

Bibliografía

Alevizos, L., & Dekker, M. (2024a). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. *Electronics*, *13*(11), 2021. https://doi.org/10.3390/electronics13112021

Alevizos, L., & Dekker, M. (2024b). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. *Electronics*, *13*(11), 2021. https://doi.org/10.3390/electronics13112021

Biagio, M. S., Acquaviva, R., Mazzonello, V., La Mattina, E., & Morreale, V. (2021). A new SOCMINT framework for Threat Intelligence Identification. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 692-697. https://doi.org/10.1109/CSCI54926.2021.00180

Böhm, I., & Lolagar, S. (2021). Open source intelligence: Introduction, legal, and ethical considerations. *International Cybersecurity Law Review*, *2*(2), 317-337. https://doi.org/10.1365/s43439-021-00042-7

Caballero-Delgadillo, J. A., Flores-Ordóñez, M., & Ledesma-Ayora, M. (2025). Inteligencia, Contrainteligencia y el Servicio del *Humint*. *Erevna Research Reports*, *3*(2), e2025020. https://doi.org/10.70171/fgtpcn17

Irfan, A. N., Chuprat, S., Mahrin, M. N., & Ariffin, A. (2022a). Taxonomy of Cyber Threat Intelligence Framework. *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 1295-1300. https://doi.org/10.1109/ICTC55196.2022.9952616

Irfan, A. N., Chuprat, S., Mahrin, M. N., & Ariffin, A. (2022b). Taxonomy of Cyber Threat Intelligence Framework. *2022 13th International Conference on*

Information and Communication Technology Convergence (ICTC), 1295-1300. https://doi.org/10.1109/ICTC55196.2022.9952616

Paya-Santos, C., & Luque-Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova*, *19*(36), 1121-1136. https://doi.org/10.21830/19006586.855

Ramírez Quevedo, L. (2024). Tecnologías de defensa frente a inteligencia de amenazas y ciberataques. *InnDev*, *3*(1), 127-141. https://doi.org/10.69583/inndev.v3n1.2024.94

Sushama Pawar, Yogita Khandagale, Archana Gopnarayan, & Manisha Pokharkar. (2024). Cyber Threat Intelligence: A Comprehensive Overview and Practical Implementation. *International Journal of Advanced Research in Science, Communication and Technology*, 529-534. https://doi.org/10.48175/IJARSCT-18179

Tang, B., & Qiu, H. (2022). Indicators of Compromise Automatic Identification Model Based on Cyberthreat Intelligence and Deep Learning. *2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI)*, 282-287. https://doi.org/10.1109/PRAI55851.2022.9904197

Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics*, *10*(12), 2054. https://doi.org/10.3390/math10122054

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, 9, 94318-94337. https://doi.org/10.1109/ACCESS.2021.3087109

Contáctenos

📧 **Correo electrónico:** csirt@unad.edu.co
🌐 **Página web:** https://csirt.unad.edu.co

🛡️ El CSIRT Académico UNAD está siempre disponible para apoyarte ante consultas o inquietudes relacionadas con la protección de la información en la universidad. No dudes en ponerte en contacto con nuestro equipo para recibir asesoría, reportar incidentes o recibir orientación en temas de seguridad digital. ¡Tu seguridad es nuestra prioridad!