ARTÍCULO DE
Revisión

sciencevolution

ISSN: 2810-8728 (En línea)

4.12
OCTUBRE - DICIEMBRE 2024

Artículo de Revisión
212 - 222

# INTELIGENCIA Y CONTRAINTELIGENCIA EN CIBERSEGURIDAD: HERRAMIENTAS CLAVE PARA LA DEFENSA DIGITAL

CYBERSECURITY INTELLIGENCE AND COUNTERINTELLIGENCE: ESSENTIAL TOOLS FOR DIGITAL DEFENSE

**Luis Soto Tejedor**
llsoto@sglegalconsulting.com
ORCID: 0009-0002-4958-1451
Investigador independiente. Abogado 47165. Ilustre Colegio de la Abogacía de Barcelona, Badalona - España

**Víctor Fernández Massó**
elenaflores@uadec.edu.mx
ORCID: 0009-0006-6952-1519
Investigador independiente. Investigador privado 6329 Policía Nacional Española, Perito Judicial en Ciencias Criminológicas, Criminalísticas y Valorativas, Prades - España

**Aceptación**: 19 de Noviembre del 2024
**Publicación**: 24 de Diciembre del 2024

## RESUMEN

Se han recopilado las herramientas tecnológicas que han demostrado mayor efectividad ante los ciberataques, sistemas empleados para acciones de inteligencia y contrainteligencia en ciberseguridad. Las tecnologías presentadas en este estudio son utilizadas en la prevención, detección y en el contrarresto de las actividades delictivas en la red; por ejemplo, la infección de software malicioso, como Spyware y Ransomware. También, se incluyen definiciones, usos y beneficios de los sistemas que ayudan a mejorar los niveles de seguridad a nivel empresarial, organizacional y para las personas que de forma cotidiana navegan en la red, con el propósito de minimizar los riesgos y promover la defensa ante las amenazas cibernéticas. Una revisión narrativa, elaborada con un método de interpretación hermenéutica, con 43 fuentes de directorios como Google Scholar, Dialnet, Scopus, entre otras. Por último, se concluye que la integración efectiva de estas disciplinas de ciberseguridad fortalecen la capacidad de defensa de las organizaciones y contribuyen al desarrollo de una cultura de prevención que valora tanto la efectividad técnica como el respeto por los derechos humanos, un enfoque holístico fundamental para abordar los desafíos complejos del panorama cibernético actual y futuro.

**Palabras clave:** Inteligencia, contrainteligencia, ciberseguridad, sistemas, ciberdelincuencia

## ABSTRACT

The tools that have proven to be most effective in combating cyberattacks, as well as systems used for intelligence and counterintelligence actions in cybersecurity, have been compiled. The technologies presented in this study are employed in the prevention, detection, and counteraction of criminal activities in digital environments, such as the infection of malicious software like spyware and ransomware. Additionally, the study includes definitions, uses, and benefits of systems that help improve security levels at the corporate, organizational, and individual levels, aiming to minimize risks and promote defense against cyber crime. A narrative review, developed using a hermeneutic interpretation method, was conducted, utilizing 43 sources from reputable directories such as Google Scholar, Dialnet, and Scopus, among others. Finally, it concludes that the effective integration of these cybersecurity disciplines strengthens organizations' defense capabilities and contributes to the development of a culture of prevention that values both technical effectiveness and respect for human rights, a holistic approach essential for addressing the complex challenges of the current and future cyber landscape.

**Keywords:** Intelligence, counterintelligence, cybersecurity, systems, cybercrime



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

sciencevolution

ISSN: 2810-8728 (En línea)

4.12
OCTUBRE - DICIEMBRE 2024

Artículo de Revisión
212 - 222



**Victor Fernández Massó**
ORCID: 0009-0006-6952-1519

**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
https://revista.sciencevolution.com/

## INTRODUCCIÓN

El desmesurado crecimiento del internet en los últimos años, ha revolucionado por completo a la humanidad, como sociedad, en sus estructuras económicas y a nivel de infraestructuras. Una transformación denominada *cyber civilization* (o por su equivalente en español "cibercultura"), que ha generado un antes y después en la manera en que nos comunicamos, cómo hacemos negocios y accedemos a la información. Todas las acciones y operaciones del vivir diario de organizaciones y personas en general se han visto impactadas por esta nueva realidad tecnológica; por ejemplo, para realizar transacciones bancarias, contratar servicios de salud, recibir educación, desarrollar gestiones empresariales, ejecutar actividades conectándose a sistemas de red, entre otras (Admass et al. , 2024).

Aunque las tecnologías de la información (TI) brindan comodidad, practicidad y rapidez en las actividades de la población mundial, esto ha conllevado a la necesidad de superar desafíos de seguridad. Uno de ellos, es el reto de la divulgación no autorizada de datos personales, producto de ciberataques, los cuales son utilizados inescrupulosamente para cometer fraudes cibernéticos, suplantando a los ciudadanos para obtener préstamos o hacer declaraciones de impuestos. Las pérdidas por año originadas por el cibercrimen para la economía mundial se aproximan a los 500.000 millones de dólares, sin contar los costos emocionales por el daño a la reputación. Algunas cifras alarmantes, son los 8.1 millones de personas que en el año 2010, han sido víctimas de robo de identidad, solo en los Estados Unidos, un número que al periodo 2018 habría incrementando a 14.4 millones de afectados (Kavak et al. , 2021); mientras que, en España, al 2023, los ciudadanos afectados por falsificación informática ascendieron a 15 137, por fraude informático 427 448 y por interferencia en datos y en sistemas 1 659 (Gobierno de España, 2023).

En consecuencia, la ciberseguridad ha adquirido una relevancia sin precedentes en la actual era digital, donde la protección de datos y redes se ha vuelto una prioridad para organizaciones e individuos. Asimismo, los llamados "ciberataques" son cada vez más eficaces y rápidos; por ello, las empresas tienen la obligación de adaptarse a la sofisticación tecnológica actual, respondiendo con celeridad para contrarrestar estos ataques, tanto los cibernéticos, que incluyen diferentes tipos de fraude; los *hacktivistas*, como por ejemplo la organización Anonymous; los terroristas cibernéticos, que propician atentados digitales a sectores fundamentales como la banca, defensa, salud, entre otros; por último los ciberespías, que cometen robos de datos en organizaciones privadas o públicas y las comercializan en el mercado negro en línea (Computing, 2023; Ardila et al., 2021).

Ahora bien, existen diferentes tipos de hackers, desde los *script kiddies*, *newbies* y *system chal lenges*, conocidos como los hackers novatos que hacen uso de kits de herramientas que encuentran en línea. Este tipo de hackers, no buscan cometer delitos, están motivados por la curiosidad y el aprendizaje de nuevos conocimientos. Por otro lado, se encuentran los denominados *crashers*, *thugs*, *crackers* y *ciberpunks*, los cuales están cualificados a nivel medio y generan problemas en nombre de la diversión, por venganza o con la finalidad de hacerse notar. También, están los *cyber predators* o pedófilos, delincuentes sexuales en línea que utilizan internet para tener relaciones sexuales desviadas con niños. Asimismo, los ladrones que se han digitalizado para efectuar sus actividades delictivas, su interés es económico y de venganza, aquí están incluidos los extorsionadores, estafadores, defraudadores, ladrones comunes y digitales. Además, están los hackers profesionales altamente calificados, denominados sombreros negros (*black hat hackers*), élites, criminales, delincuentes organizados, intermediarios de información y ladrones, quienes actúan como mercenarios a sueldo en internet con la intención de desarrollar su imperio delictivo, motivados por el beneficio económico o por venganza (Chng et al., 2022).

Adicionalmente Chng et al. (2022), menciona a los *old guards*, hackers conocidos como sombreros blancos (*white hat hackers*) y sombreros grises (*grey hat hackers* o *sneakers*), aquellos que no poseen malas intenciones, a pesar de contar con amplios conocimientos y experiencia. Estos hackers emplean códigos, scripts y herramientas de pruebas de penetración a medida para identificar las vulnerabilidades en los sistemas, por ejemplo en sitios web, software y servidores, ordenadores, dispositivos, para hallar nuevo malware utilizando *honeypots* profesionales, conocidos como herramientas de seguridad para atraer a los delincuentes y rastrearlos mediante la aplicación de técnicas ciberforenses. Es usual que los *white hat hackers* informen acerca de estas vulnerabilidades a los propietarios o las denuncien públicamente, y, en ocasiones, trabajen mano a mano de forma anónima con empresas de seguridad, la policía o con hackers de sombrero gris.

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

Las ciberamenazas, según el World Economic Forum (2024), forman parte de los riesgos más importantes que impactan en la sociedad actual. Entre estas se encuentran el Spyware y el Ransomware. El primero forma parte de las amenazas más comunes en internet, tanto para usuarios individuales como empresas, ya que puede robar información confidencial y dañar la red (Norton, 2023). Además, recopila y envía los datos personales de las víctimas a las agencias de datos, anunciantes u otros usuarios sin su conocimiento ni consentimiento. Entre la información robada se pueden encontrar códigos de identificación y de seguridad, números de tarjetas de crédito, etc. (Lysenko et al., 2020). El Ransomware, es un tipo de software malicioso que se utiliza para bloquear los datos de la víctima con un sistema de algoritmos muy fuerte, para luego pedirle una suma de dinero, generalmente en forma de Bitcoin, a cambio de desbloquear sus datos (Song et al., 2016). Esta modalidad de ataque puede resultar en la pérdida temporal o permanente de la información, disrupción de los sistemas de operaciones y pérdidas financieras (Stephen, 2017).

Por un lado, según Sancho (2021) la inteligencia aplicada en el entorno digital, también conocida como ciberinteligencia, cumple el rol de brindar información clave en procesos como la identificación de personas, intenciones, objetivos y principalmente, anticipar ataques o fallas de funcionamiento que afecten las políticas de un país o la vida de los ciudadanos. En este sentido, encontramos tres tipos de inteligencia: inteligencia estratégica, inteligencia táctica e inteligencia operacional. Por otro lado, según la Ley 12333 (2008) de los Estados Unidos, la contrainteligencia, se encarga de recopilar la información y las actividades realizadas para identificar, engañar, explotar, interrumpir o proteger contra el espionaje; es decir, no solo previene, sino que ataca al que invade estas políticas de seguridad en el espacio cibernético. Un ejemplo de herramienta que se utiliza como contrainteligencia es el sistema Honeypot, ya que no sólo distrae al atacante, sino que se protegen los datos valiosos mientras se obtienen datos relevantes para la identificación tanto del ciberataque como del atacante (Llamas, 2020).

Por ello, el trabajo conjunto de la inteligencia y la contrainteligencia es relevante en materia de prevención y respuesta a las amenazas cibernéticas, puesto que la ciberseguridad representa una condición necesaria para navegar en el entorno digital y contrarrestar las ciberamenazas. Por lo tanto, estas disciplinas no solo permiten promover el desarrollo de la ciberinteligencia, sino también aprovechar al máximo el ciberespacio (Sancho, 2021).

Desde la perspectiva del derecho, la Unión Europea (2019) reconoce la importancia de que países miembros, entre ellos España, determinen una política eficaz para la ciberseguridad, contemplando desafíos prioritarios, que engloban problemáticas como la necesidad de contar con un marco político y legislativo, directrices de financiación y gasto, a fin de suplir la carencia de una cultura ciberresiliente y mejorar la capacidad de respuesta ágil ante los ciberincidentes.

Ante lo descrito, el objetivo de este estudio es presentar una recopilación sobre las herramientas efectivas aplicadas para la inteligencia y contrainteligencia en ciberseguridad, considerando su vigencia y relevancia, abordando un análisis crítico de las funciones, aplicaciones y limitaciones. De esta manera, la presente investigación busca contribuir de manera significativa a mejorar la comprensión de las prácticas actuales y futuras de inteligencia y contrainteligencia en el ámbito de ciberseguridad, promoviendo nuevas investigaciones y fomentando un mayor interés en este campo.

## MÉTODO

### Enfoque de la revisión

El presente artículo se basa en una revisión bibliográfica de tipo narrativo con enfoque hermenéutico de la literatura académica y fuentes especializadas en ciberseguridad, inteligencia y contrainteligencia, lo cual implica compilar, analizar y sintetizar la información actualizada sobre estas temáticas, detectando los principales programas y herramientas utilizados a la fecha de la publicación de este artículo.

La metodología de revisión bibliográfica fue seleccionada para consolidar el conocimiento teórico y práctico acumulado en el campo de la ciberseguridad. Además, permite estructurar de manera óptima la información esencial dirigida a usuarios, académicos y profesionales interesados en los programas actuales de inteligencia y contrainteligencia en entornos digitales.

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Victor Fernández Massó**
ORCID: 0009-0006-6952-1519

**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
https://revista.sciencevolution.com/

### Bases de datos y fuentes de la información

Para la elaboración de este artículo, se llevaron a cabo búsquedas en diversas bases de datos científicas de prestigio. Las principales fuentes consultadas fueron Google Scholar, Dialnet y revistas indexadas en repositorios como Scopus, entre otras. Se obtuvieron un total de 43 fuentes, las cuales fueron seleccionadas debido a su reconocimiento académico y su contribución significativa al campo de estudio. La elección de los programas y herramientas analizados se basó en los siguientes criterios:

A. **Criterios de Inclusión.** Se priorizaron publicaciones de artículos, libros y reportes, con el objetivo de garantizar la actualidad de la información. Además, se seleccionaron documentos relevantes sobre inteligencia y contrainteligencia en ciberseguridad, abarcando tanto publicaciones en español como en inglés, para incorporar perspectivas locales e internacionales. Finalmente, se incluyeron revistas indexadas, libros de referencia e informes emitidos por instituciones reconocidas en el ámbito de la ciberseguridad.
B. **Criterios de Exclusión.** Se excluyeron del presente estudio aquellas publicaciones cuya temática no estuviera directamente relacionada con el objetivo del artículo. Asimismo, se descartaron documentos provenientes de fuentes no confiables. Finalmente, se consideraron algunas fuentes publicadas antes de 2021, por considerarse especialmente relevantes para la investigación.

### Estrategia de búsqueda

Las palabras clave utilizadas incluyeron combinaciones como "inteligencia" AND "ciberseguridad", "contrainteligencia" AND "counterintelligence", "cybersecurity, "cybercrime" AND "security", "cybersecurity" AND "programs", "contrainteligencia digital", y "programas de ciberseguridad". Para la búsqueda mediante palabras clave se aplicó el buscador booleano "and", el cual permite asociar un término con otro y poder encontrar fuentes que consideren ambos, de esta manera, se optimiza la búsqueda de estudios y reportes relevantes en ciberseguridad.

### Análisis y categorización de la información

**Clasificación de temas.** Para clasificar la información y los programas, se utilizó un enfoque que aborde sus funcionalidades y limitaciones. Los estudios seleccionados se agruparon en categorías de acuerdo con los siguientes temas:

- Inteligencia en ciberseguridad
- Herramientas de contrainteligencia
- Protección de redes y datos

**Limitaciones del estudio.** Se hace hincapié en la limitación de los idiomas, que al sólo incluir estudios redactados en inglés y español, pudo excluir información relevante en otras lenguas. Por último, el acceso restringido a ciertas fuentes también representó un obstáculo al no estar disponible de forma gratuita.

## DESARROLLO Y DISCUSIÓN

La inteligencia y contrainteligencia en el ámbito de ciberseguridad son disciplinas importantes para la protección de datos, sistemas y redes contra amenazas cibernéticas. Por lo tanto, ambas implican la recolección, análisis y uso de información para prever, detectar y contrarrestar actividades maliciosas. A continuación, se realiza un análisis de la efectividad y la aplicación de importantes programas y sistemas operativos en ciberseguridad y protección de redes.

### Análisis de herramientas y técnicas de inteligencia en ciberseguridad

En el ámbito de la ciberseguridad, las herramientas y técnicas de inteligencia utilizadas, se enfocan en la recolección, análisis y respuesta a amenazas. Entre los sistemas también se encuentran aquellos que detectan actividades inusuales o maliciosas en las redes, sistemas y aplicaciones, como SIEM (Security information and event management ) y IDS (Intrusion detection system). Con este tipo de software se puede identificar patrones que amenacen la seguridad mediante herramientas que ayudan a recopilar datos relacionados al tráfico de red, la actividad del sistema y las interacciones entre los usuarios. Cabe destacar que, **existen 3 programas de inteligencia**, seleccionados por su alta capacidad para detectar amenazas mediante la recolección de información:

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

**1. Cuckoo Sandbox**
Es una reconocida herramienta versátil de análisis de malware (software malicioso), el cual genera reportes detallados con información sobre el tipo y el tamaño del archivo, el tráfico de la red, la actividad y el comportamiento del sistema (Alshmarni & Alliheedi, 2023). La palabra Sandbox viene de "sandboxing", que hace referencia a una técnica utilizada para controlar los recursos, como el CPU, la memoria o los archivos que pueden ser vulnerables a ciberataques. Este control se logra mediante la creación de un entorno aislado y seguro en el que se someten a prueba programas o enlaces maliciosos (Alam, 2022). Consta de una parte de gestión y máquinas virtuales (VMs) que simulan equipos de las víctimas, imitando a un sistema real para proteger contra ataques de malware, mediante su observación y estudio de su comportamiento, antes de afectar al sistema real. (Ilić et al., 2022).

Entre sus ventajas encontramos que es gratuita, se puede tanto instalar como configurar fácilmente y tiene el respaldo de una fuerte comunidad profesional que lo utiliza. Asimismo, tiene una buena capacidad para integrarse con diferentes herramientas, puede generar gran cantidad de reportes informativos, asimismo, tiene más opciones de virtualización y una mejor compatibilidad con sistemas operativos y muestras (Ilić et al., 2022).

Sin embargo, entre sus desventajas encontramos que, dado que esta herramienta está desarrollada en Python 2, presenta algunos problemas derivados de las dependencias con paquetes diseñados en Python 3, porque no son compatibles, generando inconvenientes para aprovechar nuevas actualizaciones y estándares modernos de Python 3. Por consiguiente, se espera que con la nueva versión creada en Python 3, Cuckoo 3 proporcione un rendimiento superior. A pesar de sus limitaciones, su versión actual tiene mayor capacidad para prevenir que un malware evada el entorno de sandbox, su script en Python 2 sigue siendo más eficaz que el de Drakvuf, otra herramienta especializada para estudiar malware en entornos virtualizados (Ilić et al., 2022).

**2. HitmanPro**
Es un programa desarrollado por la empresa Surf Right Corp., que se enfoca en detectar comportamientos inusuales en el sistema (Hammadeh y Kavitha, 2023), mediante un análisis forense en tiempo real para comparar un archivo sospechoso con algún tipo de ransomware y eliminarlo (Zahoora et al., 2022).

También destaca por ser una herramienta gratuita y se caracteriza por ser efectiva en la protección contra ataques de vulnerabilidad y de malware descritos mediante lenguajes de programación de macros, como VBA (Visual Basic for Applications). Asimismo, tiene un rango de detección alto, capaz de resistir efectivamente ante ataques de malware provenientes de internet sin que ninguno pase desapercibido (Koizumi y Sasaki, 2015).

Por otro lado, entre sus desventajas se encuentra que, HitmanPro está diseñado como una herramienta de eliminación y no como un antivirus completo. En concreto, solo identifica y elimina amenazas existentes, dejando sin protección al sistema si no se tiene un antivirus que realice análisis constantes y permanentes, brindando protección en tiempo real. Por lo tanto, si solo se cuenta con HitmanPro, el sistema puede ser infectado incluso antes de realizar un escaneo (HitmanPro, s. f.).

**3. Splunk:**
Splunk es una plataforma que gestiona grandes volúmenes de datos (Big Data) facilitando la recolección y búsqueda de información generados por máquinas, que facilita la recolección y manejo de grandes volúmenes de datos generados por máquinas, permitiendo la búsqueda de información dentro de ellos. Asimismo, es ampliamente empleado en áreas como análisis empresarial y web, gestión de aplicaciones, así como en tareas relacionadas con cumplimiento y seguridad (González, 2021).

Algunos de los aspectos positivos de esta plataforma incluyen la posibilidad de crear informes analíticos empleando cuadros y gráficos interactivos que pueden compartirse. También se destaca por ser un software escalable y de sencilla implementación para las organizaciones (González, 2021).

Por otra parte, entre sus desventajas se encuentran que las empresas pequeñas o medianas deben contar con amplios recursos requeridos por Splunk, puesto que no solo es muy costoso para estas, sino que también necesita un equipo técnico lo suficientemente capacitado para trabajar con esta plataforma (Pan, 2024).

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/



En contraste, se presentan **4 programas de contrainteligencia**, los cuales fueron seleccionados por su popularidad, abundante literatura, gran capacidad para encriptar información, además de ocultar y proteger la identidad y los datos de los usuarios.

**1. Tails**
*The Amnesic Incognito Live System* o Tails, es un sistema operativo amnésico desarrollado por Debian, una distribución de Linux, que defiende la idea de la seguridad y el anonimato para poder brindar privacidad a todos en cualquier momento. Este sistema se creó para complementar a la red Tor (The Onion Router) y reforzar el anonimato de sus usuarios (Dawson & Cárdenas-Haro, 2017). Asimismo, es ideal para quienes prefieren un sistema portable que les brinde protección contra dispositivos de recopilación de datos y busquen privacidad en internet (Negi & Kar, 2020). Además, Tails fortalece la seguridad al contar con herramientas como Keepass, un sistema gestor de contraseñas y Aircrack-ng, suite de software para auditoría de seguridad de redes Wi-Fi (Milpa Digital, 2021; Reichl, s.f.; Aircrack-ng., s.f.).

Entre sus ventajas se encuentra que este programa es portable, el usuario lo puede descargar e instalar en una memoria USB, tarjeta SD o grabarlo en un disco (Anderson et al., 2018). Además, gracias a su herramienta "Nautilus Wipe" la actividad y los datos son eliminados automáticamente al apagar el programa; luego, también ofrece la opción de activar la apariencia de un sistema Windows 8 para evitar llamar la atención cuando se utiliza en lugares públicos (Dawson & Cárdenas-Haro, 2017).

Entre sus desventajas se encuentra que, al estar compuesto por varias herramientas, si una de estas falla, puede perjudicar el desempeño de todo el sistema. Asimismo, se necesita tener conocimiento técnico sobre cómo manejar este programa para poder usarlo eficientemente. Por último, este sistema no elimina los metadatos de los archivos automáticamente, pero ofrece las herramientas necesarias para hacerlo de forma manual antes de compartirlos (Dawson & Cárdenas-Haro, 2017).

**2. Whonix**
Al igual que Tails, Whonix fue desarrollado por Debian para brindar seguridad y anonimato a sus usuarios al momento de navegar en la web, sirviéndose del navegador Tor (Lundgren, 2020; Hulina, 2020) como se citó en, Batunanggar, Widjajarto, & Kurniawan, en 2024. Sin embargo, no se trata de un sistema operativo sino de un dispositivo virtual que funciona a través de sus dos herramientas: Whonix Gateway y Whonix Workstation (Ranakoti et al., 2017). Esto impide que cualquier tráfico de red salga sin pasar por Tor, protegiendo la privacidad del usuario, además de ser idóneo para periodistas y activistas. También, Whonix asegura comunicaciones sin riesgo de rastreo, y al operar en máquinas virtuales separadas, refuerza la defensa contra posibles ataques cibernéticos. Esta estructura es esencial para quienes requieren un entorno digital altamente seguro (LinuxMind, 2024).

El primero, se conecta directamente a la red de internet Tor, mientras que el segundo se conecta mediante una red interna al Gateway (De Robles et al., 2020). De esta manera las personas pueden conectarse a la red Tor y ejecutar aplicaciones para realizar actividades del día a día. (Choorod & Weir, 2021). Esto brinda una mayor seguridad ante ataques, ya que Whonix Workstation no permitirá que se revele la identidad de los usuarios. (Batunanggar, Widjajarto, & Kurniawan, 2024).

Es un sistema que sobresale porque es de código abierto y gratuito, que funciona como una máquina virtual dentro del sistema operativo que se esté utilizando. Asimismo, utiliza la red Tor para conectarse y realizar actividades sin dejar rastro de la actividad. Según Ranakoti et al. (2017), esto se debe a que el sistema no permite mostrar la dirección IP del usuario. Por último, es efectivo para prevenir que virus envíen información al ordenador (Rawat et al., 2023).

Por otro lado, la principal desventaja es su considerable tamaño en sistemas operativos como Windows, ya que el programa ocupa 1.6 GB en el disco duro de la computadora (Rawat et al., 2023).

**3. Qubes OS**
Es un sistema de seguridad multinivel (MLS) con un sistema operativo para ordenadores y portátiles basados en la virtualización y utiliza diversas máquinas virtuales (VM), entre ellas: VM de red, VM de almacenamiento, VM de servicios, VM de aplicaciones y VM administrativas/GUI (Mehrab et al., 2022). Estas máquinas funcionan como compartimentos aislados o "qubes" y son los elementos principales del modelo de seguridad del sistema, su objetivo es aislar cada una de las VMs entre ellas para mantener la seguridad al navegar, en caso la seguridad de una esté en riesgo

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

(Rutkowska, 2018). A través de su arquitectura de múltiples qubes, Qubes OS mejora significativamente la protección contra ataques informáticos y malware (Tziritas, N., s. f.).

Se distingue por ser un programa que utiliza cada máquina virtual, debido a ello, el sistema le permite a los usuarios protegerse contra la vigilancia y ocultar mejor su identidad (Kazansky & Milan, 2021). Asimismo, Las VMs poseen un nivel de aislamiento mayor, a comparación de los procesos de sistemas operativos como Windows o Linux, porque al tener un diseño más sencillo, el hipervisor se puede comunicar de forma más directa con las VMs, a diferencia de un sistema operativo tradicional, reduciendo la posibilidad de daños al sistema (Rutkowska, 2018).

Algunas desventajas incluyen que, si bien algunas de las máquinas virtuales que ofrece tienen el formato de una plantilla lista para usarse, otras van a requerir de un proceso de personalización bien elaborado. De esta manera, el sistema no garantiza la eliminación de la causa del problema, sino que según sus desarrolladores, este ha sido creado para responder a un conjunto específico de amenazas de ciberseguridad (Kazansky & Milan, 2021). Por último, el sistema ofrece una protección completa ante ataques provenientes de aplicaciones instaladas (Marx et al., 2018).

**4. Veracrypt**

Se trata de la herramienta de código abierto más popular que sirve para la protección de datos del disco duro o partición. Es compatible con sistemas como Windows, Linux y Mac OS X. Asimismo, ofrece a sus usuarios diversos algoritmos para el cifrado de datos como Serpent, Twofish o AES. La longitud de la clave es de 256 bits. Además de estos, también ofrece algoritmos *hash* como RIPEMD-160, SHA-512 y Whirlpool, que se usan junto con datos aleatorios generados por el programa en la memoria RAM (Bursać & Milosavljević, 2017).

Entre sus ventajas incluye la característica de *on-the-fly-encryption*, el cual permite cifrar los datos automáticamente justo antes de que se guarden, así como descifrarlo después de que se transfieran o se coloquen en el archivo ubicado en la unidad de almacenamiento, permitiendo una mayor facilidad para mover los archivos en el ordenador (Bursać & Milosavljević, 2017). Asimismo, también puede cifrar todo el sistema de partición, como archivos, bootloader (gestor de arranque) y los datos del usuario, y generar grandes cantidades de volúmenes con cifrado oculto. Esto agrega una capa extra de protección, asegurando que solo aquellos con la contraseña y el archivo clave puedan acceder a la información encriptada (STIC, 2022). Además, es compatible con varios formatos de unidades de almacenamiento estándar, ocultos e incluso particiones de todo el sistema operativo. (Hassan et al., 2023)

Entre sus desventajas se encuentra que, a pesar de tener una mayor movilidad de datos, al transferirlos a otra carpeta en el ordenador, la protección se pierde ya que solo están protegidos cuando están almacenados en el archivo del volumen (Bursać & Milosavljević, 2017). Además, la velocidad de cifrado va a depender de la cantidad de procesadores del servidor u ordenador que se esté utilizando; luego, tampoco protege los archivos o directorios contra ataques de malware, especialmente en una computadora infectada (Kokofi, 2020).

## Comparativa de programas de contrainteligencia

Existen varios programas de contrainteligencia diseñados para proteger a las organizaciones contra intrusiones y amenazas cibernéticas. Entre los que más destacan son Tails y Whonix. Para ello, se presenta una comparativa de sus capacidades, algoritmos de detección y prevención de intrusiones, y escenarios de uso:

Capacidades

- **Tails**: Es un sistema operativo portátil y amnésico, lo que significa que no deja rastro de la actividad una vez apagado. Permite navegar de forma anónima a través de la red Tor, asegurando el anonimato del usuario. Además, se puede ejecutar desde una memoria USB en cualquier ordenador sin modificar el disco duro (Morabito, 2023).
- **Whonix**: Funciona como una solución basada en máquinas virtuales, separando las funciones de puerta de enlace y estación de trabajo para reducir vulnerabilidades. Ofrece una configuración robusta para el anonimato, usando Tor de manera obligatoria y protegiendo contra filtraciones de DNS (Tor Project, s.f.).

## Algoritmos de detección y prevención

- Ambos sistemas dependen del anonimato que proporciona Tor, sin embargo Whonix refuerza la seguridad mediante el uso de dos capas de firewall y una arquitectura que

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Victor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

minimiza errores del usuario. Esto lo hace menos susceptible a vulnerabilidades de configuración en comparación con Tails, que prioriza la facilidad de uso (Tor Project, s.f.).

Escenarios de uso

- **Tails**: Es utilizado por activistas que buscan proteger su identidad y evitar la censura, periodistas que necesitan mantener la confidencialidad de sus fuentes y publicar de forma segura, y cualquier usuario que desee privacidad adicional en línea. Su arquitectura garantiza el anonimato al enrutar todo el tráfico a través de Tor (Milpa Digital, 2021).
- **Whonix**: Utilizado por periodistas y activistas que requieren comunicaciones seguras, usuarios que desean mantener el anonimato en línea, y desarrolladores interesados en crear aplicaciones que prioricen la privacidad. Esta herramienta proporciona un entorno que maximiza la seguridad y el anonimato de quienes la emplean (LinuxMind, 2024).

### Efectividad en la mitigación de riesgos

La efectividad de herramientas como Tails y Whonix para mitigar riesgos de seguridad y privacidad ha sido ampliamente discutida en estudios de caso y reportes. En general, estas herramientas son muy eficaces en la protección del anonimato y la prevención de la vigilancia, pero su capacidad depende del contexto en que se usen y de la habilidad del usuario.

Según un estudio de Batunanggar et al. (2024), se evalúa la efectividad de Whonix para proteger la privacidad y el anonimato a través de aspectos como el cifrado de datos, la protección de metadatos y la compatibilidad con Tor. Los resultados muestran una alta efectividad del 97% en la protección del sistema, utilizando métricas específicas para aplicaciones, red y sistema operativo. Estas herramientas demuestran ser eficaces para minimizar los riesgos asociados con la privacidad y el anonimato en línea.

A su vez, Dawson y Cárdenas-Haro (2017), mencionan que el sistema Tails, al complementar a Tor, se presenta como una herramienta poderosa para contrarrestar la vigilancia gubernamental. A pesar de algunas limitaciones, ha demostrado ser altamente efectivo en la protección de la privacidad y en la defensa de la democracia. Su desarrollo continúa avanzando significativamente en la dirección correcta.

## CONCLUSIONES

Las organizaciones de gobierno, el sector privado y las personas deben adoptar una cultura de prevención ante los inminentes ciberataques que los hackers de sombrero negro y otros tipos de ciberdelincuentes cometen a diario en la red. Esto implica implementar programas de inteligencia, como los mencionados en este estudio, Cuckoo Sandbox, HitmanPro y Splunk, los cuales son altamente efectivos y, son considerados por los profesionales como los más relevantes. Aunque, algunos de ellos son programas gratuitos, también se debe tener en cuenta la inversión asociada a su instalación, monitoreo y mantenimiento. De esta manera, se pueden compilar los patrones de comportamiento de los que cometen los delitos cibernéticos, detectar de forma oportuna las vulnerabilidades en los sistemas y redes y, contribuir de forma significativa a la protección tanto de datos como de redes. Además, al recolectar y analizar la información crítica, se identifican conductas digitales anómalas o maliciosas, como los accesos no autorizados y actividades de malware.

Las herramientas como Splunk y Cuckoo Sandbox ayudan a mitigar los posibles ataques en la ciberred. Además, softwares como HitmanPro, detectan de forma inmediata los archivos maliciosos que se están ejecutando, ayudando a prevenir la dispersión de malware, es decir, evita que el malware se propague, mientras Splunk se encarga de monitorear y alertar en tiempo real cuando suceden eventos de seguridad.

También, saber qué herramienta es la más idónea cuando se trata de inteligencia y contrainteligencia en ciberseguridad, depende de las preferencias profesionales de los hackers de sombrero blanco, gris, o de áreas de seguridad en las organizaciones públicas o privadas. No obstante, es indispensable tener conocimiento de los requisitos específicos de cada usuario y del proyecto u operación que se desea realizar para saber cual de ellos es el que va acorde con la necesidad. Este enfoque, basado en la ciberseguridad, permite una respuesta más ágil y efectiva ante incidentes, respondiendo a una mejora significativa en la postura de seguridad general.

sciencevolution
ISSN: 2810-8728 (En línea)
4.12
OCTUBRE - DICIEMBRE 2024
Artículo de Revisión
212 - 222



**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451
**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

https://revista.sciencevolution.com/

Cabe resaltar que estas herramientas, combinadas con un enfoque proactivo, permiten la mitigación de riesgos antes de que se materialicen en ataques reales.

Aunque este estudio aborda con un carácter técnico, también ha explicado de forma clara y precisa las principales herramientas de defensa digital que los ciudadanos y todo responsable de seguridad en una organización debe conocer con la finalidad de tomar la iniciativa para proteger su identidad, fortalecer la seguridad de la infraestructura digital y reducir las brechas de datos y minimizar la frecuencia de los ciberataques.

En ese sentido, conocer y mantenerse actualizado en esta área es un primer paso para estar por delante de los atacantes digitales, permitiendo anticiparse ante las amenazas y gestionar eficazmente los riesgos asociados con el entorno online; por un lado, aprendiendo acerca de los sistemas de inteligencia y, por otro lado, descubriendo los sistemas operativos empleados en contrainteligencia para la ciberseguridad.

La ciberseguridad también plantea desafíos éticos y legales que no deben omitirse, por esta razón, es necesario encontrar el equilibrio entre la seguridad y la protección de las libertades civiles, aspectos críticos que deben considerarse en el desarrollo e implementación de estas de la inteligencia y contrainteligencia. Por ejemplo, la recolección de datos, aunque es determinante para la defensa, puede generar conflictos legales con los derechos a la privacidad de todo ciudadano.

Por lo tanto, es obligación de las organizaciones desarrollar políticas claras y directrices éticas que se apliquen a la inteligencia cibernética, promoviendo la transparencia y la rendición de cuentas en la información. La colaboración interdisciplinaria entre ciberseguridad, derecho y ética es esencial para establecer marcos que permitan un uso responsable de la inteligencia en la defensa cibernética.

Por último, la integración de la inteligencia y contrainteligencia en ciberseguridad no solo ayuda a mejorar la capacidad de defensa de las organizaciones, sino que también contribuye a desarrollar una cultura de seguridad, cuyos valores se dirigen tanto la efectividad técnica como el respeto por los derechos humanos. Este enfoque holístico es fundamental cuando se trata de abordar los desafíos complejos de la realidad cibernética vigente y futura.

## REFERENCIAS

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Aircrack-ng. (s.f.). https://www.aircrack-ng.org/

Alam, S. (2022). Cybersecurity: Past, present and future. arXiv preprint arXiv:2207.01227. https://doi.org/10.48550/arXiv.2207.01227

Anderson, J. C., Skare, E., & Dorroll, C. (2018). Nothing to hide, nothing to fear? Tools and suggestions for digital data protection. *The Qualitative Report*, *23*(5), 1223–1236. https://doi.org/10.46743/2160-3715/2018.3328

Ardila Osma, J. A., Salcedo González, E. F., Pedraza Aguirre, C. A., & Saavedra, M. (2021). Revisión sobre hacking ético y su relación con la inteligencia artificial. *Reto*, *8*(1), 11–21. https://doi.org/10.23850/reto.v8i1.3064

Batunanggar, Y. J. S., Widjajarto, A., & Kurniawan, M. T. (2024). Implementation and analysis of profiling mechanism for anonymity and privacy on Whonix operating system. *Journal of Information System Research (JOSH)*, *6*(1), 23–33. https://ejurnal.seminar-id.com/index.php/josh/article/view/5682

Bursać, M., Vulović, R., & Milosavljević, M. (2017). Comparative analysis of the open source tools intended for data encryption. *Information Technology and Education Development - ITRO*. https://www.researchgate.net/publication/320703072_Comparative_Analysis_of_the_Open_Source_Tools_Intended_for_Data_Encryption

Choorod, P., & Weir, G. (2021). Tor traffic classification based on encrypted payload characteristics. En *2021 National Computing Colleges Conference (NCCC)*. 1–6. IEEE. https://doi.org/10.1109/NCCC49330.2021.9428874

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Computing. (29 de noviembre de 2023). La IA avanzada y la contrainteligencia de amenazas combatirán el nuevo cibercrimen. *Digital 360 Iberia*. https://www.computing.es/noticias/la-ia-avanzada-y-la-contrainteligencia-de-amenazas-combatiran-el-nuevo-cibercrimen/

sciencevolution

ISSN: 2810-8728 (En línea)

4.12
OCTUBRE - DICIEMBRE 2024

Artículo de Revisión
212 - 222



**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451

https://revista.sciencevolution.com/

Dawson, M., & Cárdenas-Haro, J. A. (2017). Tails Linux operating system: Remaining anonymous with the assistance of an incognito system in times of high surveillance. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, *1*(1), 47–55. https://doi.org/10.4018/IJHIoT.2017010104

De Robles, M. B., Hermocilla, J. A. C., & Pabico, J. P. (2020). Characterization and classification of malware traffic over the Tor network. In *Proceedings of Philippine Computing Science Congress*. 78–88. https://jachermocilla.org/publications/derobles-pcsc2020-characterization.pdf

Gobierno de España. (2023). Informe sobre la cibercriminalidad en España. Ministerio del Interior. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf

González de Juana, O. (2021). Generación de ciberinteligencia con Splunk [Tesis de grado, Universidad Politécnica de Valencia]. *Repositorio Institucional RiuNet*. http://hdl.handle.net/10251/174443

Hassan Abdullahi, Z., Singh, S. K., & Hasan, M. (2023). Software reverse engineering techniques for evaluating anti-forensic encryption tools: A framework development and analysis. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(1S), 620–632. https://ijisae.org/index.php/IJISAE/article/view/3497

HitmanPro. (s. f.). HitmanPro. *Advanced malware scanning and removal with Hitman Pro*. https://www.hitmanpro.com/en-us/hmp

Ilić, S. Ž., Gnjatović, M. J., Popović, B. M., & Maček, N. D. (2022). A pilot comparative analysis of the Cuckoo and Drakvuf sandboxes: An end-user perspective. *Vojnotehnički glasnik/Military Technical Courier*, *70*(2), 372-392. https://www.redalyc.org/journal/6617/661772309007/661772309007.pdf

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. *Journal of Cybersecurity*, *7*(1), tyab005. https://doi.org/10.1093/cybsec/tyab005

Kazansky, B., & Milan, S. (2021). "Bodies not templates": Contesting dominant algorithmic imaginaries. *New Media & Society*, *23*(2), 363–381. https://doi.org/10.1177/1461444820929316

Kokofi, C. K. (2020). *Leveraging users to break cyber kill chain* (Master's thesis, University of Turku, Department of Future Technologies). https://www.utupub.fi/bitstream/handle/10024/148827/thesis.pdf?sequence=1

LinuxMind. (15 de mayo de 2024). *Guía completa del SO Whonix: Cómo funciona, orientación y curiosidades*. LinuxMind. https://linuxmind.dev/2024/05/15/guia-completa-del-so-whonix-como-funciona-orientacion-y-curiosidades/

Llamas Covarrubias, J. Z. (12 de marzo de 2020). Las tres "C" de los Estados contemporáneos: Ciberespacio, ciberseguridad y contrainteligencia. *SSRN*. http://dx.doi.org/10.2139/ssrn.3649221

Lysenko, S., Bobrovnikova, K., Popov, P. T., Kharchenko, V., & Medzatyi, D. (2020). Spyware detection technique based on reinforcement learning. *CEUR Workshop Proceedings*, 2623, 307–316. https://ceur-ws.org/Vol-2623/paper26.pdf

Marx, M., Sy, E., Burkert, C., & Federrath, H. (2018). Anonymity online: Current solutions and challenges. En: M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), *Privacy and identity management: The smart revolution. Privacy and identity 2017* (526), 38–55. Springer. https://doi.org/10.1007/978-3-319-92925-5_4.

Mehrab, A. K. M. F., Nikolaev, R., & Ravindran, B. (2022). Kite: Lightweight critical service domains. *Proceedings of the 17th European Conference on Computer Systems (EuroSys '22)*, 384 - 401, Rennes, France. ACM. https://doi.org/10.1145/3492321.3519586

Milpa Digital. (2021). *Revista Milpa Digital: Edición 59*. https://milpadigital.org/wp-content/uploads/2021/07/MilpaDigital-59-color.pdf

Morabito, D. (1 de septiembre de 2023). Tails: sistema operativo amnésico y privado. Protege.LA. https://protege.la/guias-contenido/tails-sistema-operativo-amnesico-y-privado/

Negi, V. S., & Kar, N. (2020). Security and anonymity aspects in Tails and Windows 10 operating systems. In N. Kar, A. Saha, & S. Deb (Eds.), *Trends in computational intelligence, security and internet of things: ICCISIoT 2020*, (1358), 188–199. *Springer* https://doi.org/10.1007/978-3-030-66763-4_17

sciencevolution

ISSN: 2810-8728 (En línea)

4.12
OCTUBRE - DICIEMBRE 2024

Artículo de Revisión
212 - 222



**Víctor Fernández Massó**
ORCID: 0009-0006-6952-1519

**Luis Soto Tejedor**
ORCID: 0009-0002-4958-1451

https://revista.sciencevolution.com/

Norton. (23 de julio de 2023). What is spyware? And how to remove it. https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

Pan, X. (2024). Independent study of splunk. *OAlib*, *11*(4), 1–16. https://www.scirp.org/journal/paperinformation?paperid=132789

Ranakoti, P., Yadav, S., Apurva, A., Tomer, S., & Roy, N. R. (2017). Deep web & online anonymity. In *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, 215–219. https://doi.org/10.1109/ic3tsn.2017.8284479

Rawat, M. A., Mehlawat, M. M., & Garg, M. N. (2023). Achieving anonymity with the help of TOR (TOR: A review). *International Journal of Advances in Engineering and Management (IJAEM)*, *5*(4), 778–785. https://ijaem.net/issue_dcp/Achieving%20Anonymity%20with%20the%20helpof%20TOR%20(TOR%20A%20Review).pdf

Reichl, D. (s.f.). KeePass Password Safe. https://keepass.info/

Rutkowska, J. (22 de enero 2018). Qubes Air: Generalizing the Qubes Architecture. *Invisible Things Lab Tech Report*. https://www.qubes-os.org/news/2018/01/22/qubes-air/

Sancho Hirane, C. (2021). Ciberinteligencia: Contextualización, aproximación conceptual, características y desafíos. *Cuaderno de Trabajo*, (1), 1-32. https://www.publicacionesanepe.cl/index.php/cdt/article/view/911

Song, S., Kim, B., & Lee, S. (2016). The effective ransomware prevention technique using process monitoring on Android platform. *Mobile Information Systems*,(1), https://doi.org/10.1155/2016/2946735

Stephen, J. (2017). Beware the ransomware: Protecting your data more important than ever. *Wisconsin Law Journal*. *https://wislawjournal.com/2017/05/17/beware-the-ransomware-protecting-your-data-more-important-than-ever/*

STIC. (7 de noviembre de 2022). Proteger los medios USB con una contraseña a través de VeraCrypt. *Ciberseguridad*. https://ciberseguridad.comillas.edu/mediosusb-veracrypt/

Tor Project. (s.f.). *About Tor Browser*. Tor Project. https://tb-manual.torproject.org/es/about/

Unión Europea. (2019). Desafíos de una política eficaz de ciberseguridad en la UE. Tribunal de Cuentas Europeo. https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_es.pdf

Tziritas, N. (s.f.). *Secure operating systems* [Archivo PDF]. Universidad de Tesalia. Recuperado de https://eclass.uth.gr/modules/document/file.php/DIB_P_113/Lectures/Lecture9.pdf

World Economic Forum. (10 de enero de 2024). *Global Risks Report 2024*. https://www.weforum.org/publications/global-risks-report-2024/